

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001年10月11日 (11.10.2001)

PCT

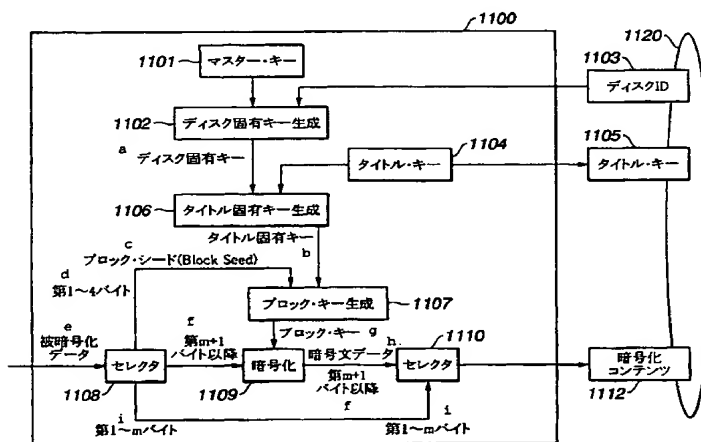
(10) 国際公開番号
WO 01/76127 A1

- (51) 国際特許分類⁷: H04L 9/00, G11B 20/10, 20/12 (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- (21) 国際出願番号: PCT/JP01/02928
- (22) 国際出願日: 2001年4月4日 (04.04.2001) (72) 発明者; および (75) 発明者/出願人 (米国についてのみ): 浅野智之 (ASANO, Tomoyuki) [JP/JP]. 大澤義知 (OSAWA, Yoshitomo) [JP/JP]. 加藤元樹 (KATO, Motoki) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 特願2000-101862 2000年4月4日 (04.04.2000) JP (74) 代理人: 小池 晃, 外(KOIKE, Akira et al.); 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo (JP).
特願2000-243207 2000年8月10日 (10.08.2000) JP

[続葉有]

(54) Title: INFORMATION RECORDING/REPRODUCING APPARATUS AND METHOD

(54) 発明の名称: 情報記録/再生装置及び方法



1101...MASTER KEY
1102...CREATION OF DISK UNIQUE KEY
a...DISK UNIQUE KEY
1104...TITLE KEY
1106...CREATION OF TITLE UNIQUE KEY
b...TITLE UNIQUE KEY
c...BLOCK SEED
d...FIRST TO FOURTH BYTES
1107...CREATION OF BLOCK KEY
e...DATA TO BE CIPHERED
1108...SELECTOR
f... (m+1)-TH AND LATER BYTES
1109...CIPHERING
g...BLOCK KEY
h...CIPHERED TEXT DATA
1110...SELECTOR
i...FIRST TO m-TH BYTES
1103...DISK ID
1105...TITLE KEY
1112...CIPHERED CONTENT

(57) Abstract: A block key for ciphering block data by using ATS added depending on the arrival time of a transport packet constituting a transport stream is created. Since the ATS is random data depending on the time, a unique key different with block can be created, thereby enhancing the strength against cipher analysis. The block key is created by combining the ATS and keys unique to the device and the recording medium such as the master key, disk unique key, and title unique key. Since the block key is created using the ATS, no areas on the recording medium for storage of a ciphering key for each block is required.

[続葉有]



(81) 指定国 (国内): AU, CN, ID, IN, KR, MX, RU, SG, US.

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:

— 国際調査報告書

(57) 要約:

トランスポートストリームを構成するランスポートパケットの着信時刻に応じて付加されるA T Sを用いてブロック・データを暗号化するブロックキーを生成する。A T Sは時刻に応じたランダムなデータであるので、ブロック毎に異なる固有キーを生成でき、暗号解析に対する強度が高まる。ブロックキーは、A T Sと、マスターキー、ディスク固有キー、タイトル固有キー等、デバイス、記録媒体に固有の鍵を組み合わせて生成する。A T Sを用いてブロックキーを生成することにより、ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となる。

明細書

情報記録／再生装置及び方法

技術分野

本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法及び情報記録媒体、並びにプログラム提供媒体に関し、特に、データ記録再生可能な記録媒体に対するデータ書き込み、データ再生処理における違法コピーを防止することを可能とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、及び情報記録媒体、並びにプログラム提供媒体に関する。

背景技術

ディジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、ディジタル的に記録する記録装置や記録媒体が普及しつつある。このようなディジタル記録装置及び記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにディジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなディジタルデータの不正なコピーを防ぐため、ディジタル記録装置及び記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

例えば、MD（ミニディスク）（MDは商標）装置において、違法なコピーを防止する方法として、SCMS（Serial Copy Management System）が採用されている。SCMSは、データ再生側において、オーディオデータとともにSCMS信号をディジタルインタフェース（DIF）から出力し、データ記録側において、

再生側からのSCMS信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

具体的にはSCMS信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー (copy free) のデータであるか、1度だけコピーが許されている (copy once allowed) データであるか、又はコピーが禁止されている (copy prohibited) データであるかを表す信号である。データ記録側において、DIFからオーディオデータを受信すると、そのオーディオデータとともに送信されるSCMS信号を検出する。そして、SCMS信号が、コピーフリー (copy free) となっている場合には、オーディオデータをSCMS信号とともにミニディスクに記録する。また、SCMS信号が、コピーを1度のみ許可 (copy once allowed) となっている場合には、SCMS信号をコピー禁止 (copy prohibited) に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、SCMS信号が、コピー禁止 (copy prohibited) となっている場合には、オーディオデータの記録を行わない。このようなSCMSを使用した制御を行うことで、ミニディスク装置では、SCMSによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

しかしながら、SCMSは上述のようにSCMS信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、SCMSの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、DVDプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

コンテンツ・スクランブルシステムでは、DVD-ROM (Read Only Memory) に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー (復号鍵) が、ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画

像や音声を再生することができる。

一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するためのキーを有していないため、DVD-ROMに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、デジタルデータを記録したDVD-ROMの再生を行えないことになり、不正コピーが防止されるようになっている。

しかしながら、DVD-ROMで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ROMメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、RAMメディアという）への適用については考慮されていない。

即ち、ROMメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、RAMメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

そこで、本出願人は、先の特許出願、特開平11-224461号公報（特願平10-25310号）において、個々の記録媒体を識別するための情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受けの際、不正な複製（違法コピー）ができないように、その動作が規定される。

ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けてい

ない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

ところで、特開平 1 1 - 2 2 4 4 6 1 号公報（特願平 1 0 - 2 5 3 1 0 号）において開示している構成は、ディスクに記録する画像、音声、プログラム等のコンテンツデータを各セクタ毎に個別の鍵セクタキーを用いて暗号化する構成としている。

これは、1つの暗号鍵で大量のデータを暗号化すると、媒体上に格納された暗号文と、何らかの手段で攻撃者が入手した平文の組を用いて、差分攻撃や線形攻撃などの暗号攻撃の手法により、暗号鍵が露呈しやすくなるという課題に対処するためである。上記の出願ではセクタという決まった大きさ毎に暗号鍵を変えることにより、1つの暗号鍵で処理するデータの量を小さく抑さえて暗号鍵の解読を困難にすることができる。さらに、万が一鍵が解読された場合においても復号可能なデータ量を少なくすることができる。

しかしながら、上記公報に記載の例では、コンテンツの暗号化に使用したセクタ毎の暗号鍵（セクタキー）をさらに上位の鍵で暗号化して、記録媒体のセクタヘッダに格納している。このため、セクタヘッダに暗号化したセクタキーを格納するだけの領域が必要になり、また、コンテンツの記録、再生時に、メインデータ部だけでなく、セクタヘッダにアクセスをして暗号化セクタキーの書き込み（記録時）もしくは読出し（再生時）を行わなければならない。

発明の開示

本発明は、上述のような従来技術の問題点を解決することを目的とするものであり、ブロックデータの暗号化処理を異なる鍵で実行可能として暗号解析に対する強度を高めることができる構成とするとともに、暗号鍵の格納領域をディスク上に新たに設ける必要を排除してデータ領域を狭めることのない構成を実現する

情報記録装置、情報再生装置、情報記録方法、情報再生方法、及び情報記録媒体、並びにプログラム提供媒体を提供する。

より、具体的には、本発明は、データを構成するトランスポートストリームに含まれる各パケットの着信時刻に応じたランダム性のあるデータとして構成されるATSを用いてブロック・データを暗号化するブロックキーを生成する構成としてブロック毎に異なる固有キーを生成することで、暗号解析に対する強度を高め、また、ATSを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域を不要としてメインデータ領域を有効に使用可能とする情報記録装置、情報再生装置、情報記録方法、情報再生方法、及び情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

上述した目的を達成する本発明の第1の側面は、記録媒体に情報を記録する情報記録装置において、間欠的なトランスポートパケットからなるトランスポートストリームを構成する各パケットに受信時刻情報（ATS）を付加するトランスポート・ストリーム処理手段と、前記受信時刻情報（ATS）の付加された1以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報（ATS）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理手段と、を有し、前記暗号処理手段によって暗号化したデータを前記記録媒体に記録する構成としたことを特徴とする情報記録装置にある。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報（ATS）を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する暗号処理用のブロックキーを生成する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基

づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとを生成して前記記録媒体に格納する処理を実行する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記ブロックシードは、前記受信時刻情報（ATS）の他にコピー制御情報を含むデータであることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記ブロックデータの暗号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより暗号化する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、該暗号処理手段を構成するLSIに格納されたLSIキー、前記情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組

合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する暗号処理用のブロックキーを生成する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記ブロックデータに対するブロックキーによる暗号処理をDESアルゴリズムに従って実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする。

さらに、本発明の第2の側面は、記録媒体から情報を再生する情報再生装置において、前記記録媒体に記録された暗号データを復号する暗号処理手段であり、複数のトランスポートパケットの各々に受信時刻情報(ATS)を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する暗号処理手段と、前記暗号処理手段において復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報(ATS)に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段と、を有することを特徴とする情報再生装置にある。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報(ATS)を含むブロックデータ固有

の付加情報であるブロックシードに基づいて、前記ブロックデータに対する復号処理用のブロックキーを生成する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記ブロックシードは、前記受信時刻情報（ATS）の他にコピー制御情報を含むデータであることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記ブロックデータの復号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより復号する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、該暗号処理手段を構成するLSIに格納されたLSIキー、前記情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒

体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組合せに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する復号処理用のブロックキーを生成する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記ブロックデータに対するブロックキーによる復号処理をDESアルゴリズムに従って実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、記録媒体からの再生対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて再生実行の可否を制御する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、記録媒体からの再生対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、コピーを制御するためのコピー制御情報としての2ビットのEMI(Encryption Mode Indicator)を識別し、該EMIに基づいて再生実行の可否を制御する構成を有することを特徴とする。

さらに、本発明の第3の側面は、記録媒体に情報を記録する情報記録方法において、トランスポートパケットからなるトランスポートストリームを構成する各パケットに受信時刻情報(ATS)を付加するトランスポート・ストリーム処理ステップと、前記受信時刻情報(ATS)の付加された1以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理ステップと、を有し、前記暗号処理ステップによって暗号化したデータを前記記録媒体に記録することを特徴とする情報記録方法にある。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報(ATS)を含むブロックデータ

固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する暗号処理用のブロックキーを生成することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとを生成して前記記録媒体に格納する処理を実行する識別子生成ステップを有することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記ブロックデータの暗号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより暗号化することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、暗号処理手段を構成するLSIに格納されたLSIキー、情報記録装置に格

納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する暗号処理用のブロックキーを生成することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記ブロックデータに対するブロックキーによる暗号処理をDESアルゴリズムに従って実行することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御するコピー制御ステップを有することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、コピーを制御するためのコピー制御情報としての2ビットのEMI(Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体に対する記録実行の可否を制御するコピー制御ステップを有することを特徴とする。

さらに、本発明の第4の側面は、記録媒体から情報を再生する情報再生方法において、複数のトランスポートパケットの各々に受信時刻情報(ATS)を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する復号処理ステップと、前記暗号処理ステップにおいて復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報(ATS)に基づいてデータ出力制御を実行するトランスポート・ストリーム処理ステップと、を有することを特徴とする情報再生方法にある。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する

復号処理用のブロックキーを生成することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記ブロックデータの復号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより復号することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、暗号処理手段を構成するLSIに格納されたLSIキー、情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する復号処理用のブロックキーを生成することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記ブロックデータに対するブロックキーによる復号処理をDESアルゴリズムに従って実行することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体からの情報再生実行の可否を制御するコピー制御ステップを有することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、コピーを制御するためのコピー制御情報としての2ビットのEMI(Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体からの情報再生実行の可否を制御するコピー制御ステップを有することを特徴とする。

さらに、本発明の第5の側面は、トランスポートストリームを構成する各パケットに受信時刻情報(ATS)を付加した1以上のパケットからなるブロックデータの暗号化鍵として使用されるブロックキーの生成情報となる受信時刻情報(ATS)を含むブロックシードを有する非暗号化データ部と、前記ブロックキーにより暗号化された暗号化データ部と、を構成要素とするブロックデータを記録したことを特徴とする記録媒体にある。

さらに、本発明の第6の側面は、記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、間欠的なトランスポートパケットからなるトランスポートストリームを構成する各パケットに受信時刻情報(ATS)を付加するトランスポート・ストリーム処理ステップと、前記受信時刻情報(ATS)の付加された1以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理ステップと、を有することを特徴とするプログラム提供媒体にある。

さらに、本発明の第7の側面は、記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供する

プログラム提供媒体であって、前記コンピュータ・プログラムは、複数のトランスポートパケットの各々に受信時刻情報（A T S）を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報（A T S）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する復号処理ステップと、前記暗号処理ステップにおいて復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（A T S）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理ステップと、を有することを特徴とするプログラム提供媒体にある。

本発明においては、記録媒体に記録するコンテンツの形式をM P E G 2 T S パケット（p a c k e t）とし、このパケットを記録装置が受信した時刻情報であるA T Sを付加して記録する。A T Sは24乃至32ビットのデータであり、ある程度のランダム性がある。ここで、A T SはArrival Time Stamp（着信時刻スタンプ）の略である。

記録媒体のひとつのブロック（セクタ）には、A T Sを付加したT S パケットをX個記録することにし、その第1番目のT S パケットに付加されたA T Sを用いてそのブロックのデータを暗号化するブロックキーを生成する。

このようにすることにより、各ブロック毎に固有の鍵を用いて暗号化することができ、また鍵を格納する特別な領域も不要となり、記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなる。

さらに、T S パケットにA T Sだけでなくコピー制限情報（C C I : Copy Control Information）も付加して記録し、A T SとC C Iを用いてブロックキーを生成するようにすることも可能である。

なお、本発明の第6及び第7の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、C D や F D、M O などの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピ

ュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

図面の簡単な説明

図 1 は、本発明の情報記録再生装置の構成例（その 1）を示すブロック図である。

図 2 は、本発明の情報記録再生装置の構成例（その 2）を示すブロック図である。

図 3 A 及び図 3 B は、本発明の情報記録再生装置のデータ記録処理フローを示す図である。

図 4 A 及び図 4 B は、本発明の情報記録再生装置のデータ再生処理フローを示す図である。

図 5 は、本発明の情報記録再生装置において処理されるデータフォーマットを説明する図である。

図 6 は、本発明の情報記録再生装置におけるトランスポート・ストリーム（T S）処理手段の構成を示すブロック図である。

図 7 A～図 7 C は、本発明の情報記録再生装置において処理されるトランスポート・ストリームの構成を説明する図である。

図 8 は、本発明の情報記録再生装置におけるトランスポート・ストリーム（T S）処理手段の構成を示すブロック図である。

図 9 は、本発明の情報記録再生装置におけるトランスポート・ストリーム（T S）処理手段の構成を示すブロック図である。

図 10 は、本発明の情報記録再生装置において処理されるブロックデータの付

加情報としてのブロック・データの構成例を示す図である。

図 1 1 は、本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その 1）である。

図 1 2 は、本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その 2）である。

図 1 3 は、本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ記録処理時の暗号化処理を説明するフローチャートである。

図 1 4 は、本発明の情報記録再生装置におけるブロック・キーの生成方法を説明する図である。

図 1 5 は、本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ再生処理時の復号処理を説明するブロック図である。

図 1 6 は、本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ再生処理時の復号処理を説明するフローチャートである。

図 1 7 は、本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図である。

図 1 8 は、本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデータ記録処理時の暗号化処理を説明するフローチャートである。

図 1 9 は、本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデバイス固有キー生成処理例（その 1）を説明するブロック図である。

図 2 0 は、本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデバイス固有キー生成処理例（その 2）を説明するブロック図である。

図 2 1 は、本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデータ再生処理時の復号処理を説明するブロック図である。

図 2 2 は、本発明の情報記録再生装置において、データ互換性の要請されない

システムにおけるデータ再生処理時の復号処理を説明するフローチャートである。

図 2 3 は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その 1）である。

図 2 4 は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その 2）である。

図 2 5 は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理を説明するフローチャートである。

図 2 6 は、本発明の情報記録再生装置におけるディスク固有キーの生成例を説明する図である。

図 2 7 は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるタイトル固有キーの生成処理フローを示す図である。

図 2 8 は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録時のタイトル固有キーの生成処理例を示す図である。

図 2 9 は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理時の復号処理を説明するブロック図である。

図 3 0 は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理を説明するフローチャートである。

図 3 1 は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理における再生可能制判定処理の詳細を示すフローチャートである。

図 3 2 は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ最盛時のタイトル固有キーの生成処理フローを示す図である。

図 3 3 A 及び図 3 3 B は、本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

図 3 4 A 及び図 3 4 B は、本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

図 3 5 は、本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

発明を実施するための最良の形態

[システム構成]

図1は、本発明を適用した記録再生装置100の一実施例形態の構成を示すブロック図である。記録再生装置100は、入出力I/F(Interface)120、MPEG(Moving Picture Experts Group)コーデック130、A/D、D/Aコンバータ141を備えた入出力I/F(Interface)140、暗号処理手段150、ROM(Read Only Memory)160、CPU(Central Processing Unit)170、メモリ180、記録媒体195のドライブ190、さらにトランスポート・ストリーム処理手段(TS処理手段)300を有し、これらはバス110によって相互に接続されている。

入出力I/F120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力I/F140に出力するとともに、入出力I/F140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力I/F140は、A/D、D/Aコンバータ141を内蔵している。入出力I/F140は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A/D、D/Aコンバータ141でA/D(Analog Digital)変換することで、デジタル信号として、MPEGコーデック130に出力するとともに、MPEGコーデック130からのデジタル信号を、A/D、D/Aコンバータ141でD/A(Digital Analog)変換することで、アナログ信号として、外部に出力する。

暗号処理手段150は、例えば、1チップのLSI(Large Scale Integrated Circuit)で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号を暗号化し、又は復号し、バス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェア又はハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構

成による処理手段としての構成については後段で説明する。

R O M 1 6 0 は、例えば、記録再生装置毎に固有の、あるいは、複数の記録再生装置のグループ毎に固有のデバイスキーを記憶している。C P U 1 7 0 は、メモリ 1 8 0 に記憶されたプログラムを実行することで、M P E G コーデック 1 3 0 や暗号処理手段 1 5 0 等を制御する。メモリ 1 8 0 は、例えば、不揮発性メモリで、C P U 1 7 0 が実行するプログラムや、C P U 1 7 0 の動作上必要なデータを記憶する。ドライブ 1 9 0 は、デジタルデータを記録再生可能な記録媒体 1 9 5 を駆動することにより、記録媒体 1 9 5 からデジタルデータを読み出し（再生し）、バス 1 1 0 上に出力するとともに、バス 1 1 0 を介して供給されるデジタルデータを、記録媒体 1 9 5 に供給して記録させる。なお、プログラムを R O M 1 6 0 に、デバイスキーをメモリ 1 8 0 に記憶するように構成してもよい。

記録媒体 1 9 5 は、例えば、D V D、C D 等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいは R A M 等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ 1 9 0 に対して着脱可能な構成であるとする。但し、記録媒体 1 9 5 は、記録再生装置 1 0 0 に内蔵する構成としてもよい。

トランスポート・ストリーム処理手段（T S 処理手段）3 0 0 は、後段において図 6 以下を用いて詳細に説明するが、例えば複数の T V プログラム（コンテンツ）が多重化されたトランスポートストリームから特定のプログラム（コンテンツ）に対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体 1 9 5 に格納するためのデータ処理及び、記録媒体 1 9 5 からの再生処理時の出現タイミング制御処理を行う。

トランスポートストリームには、各トランスポートパケットの出現タイミング情報としての A T S（Arrival Time Stamp：着信時刻スタンプ）が設定されており、このタイミングは M P E G 2 システムズで規定されている仮想的なデコーダである T - S T D（Transport stream System Target Decoder）を破綻させないように符号化時に決定され、トランスポートストリームの再生時には、各トラ

ンспорт packets に付加された A T S によって出現タイミングを制御する。トランスポート・ストリーム処理手段 (T S 処理手段) 3 0 0 は、これらの制御を実行する。例えば、トランスポート packets を記録媒体に記録する場合には、各 packets の間隔を詰めたソース packets として記録するが、各トランスポート packets の出現タイミングを併せて記録媒体に保存することにより、再生時に各 packets の出力タイミングを制御することが可能となる。トランスポート・ストリーム処理手段 (T S 処理手段) 3 0 0 は、 D V D 等の記録媒体 1 9 5 へのデータ記録時に、各トランスポート packets の入力タイミングを表す A T S (Arrival Time Stamp : 着信時刻スタンプ) を付加して記録する。

本発明の記録再生装置 1 0 0 は、上述の A T S の付加されたトランスポートストリームによって構成されるコンテンツについて、暗号処理手段 1 5 0 において暗号化処理を実行し、暗号化処理のなされたコンテンツを記録媒体 1 9 5 に格納する。さらに、暗号処理手段 1 5 0 は、記録媒体 1 9 5 に格納された暗号化コンテンツの復号処理を実行する。これらの処理の詳細については、後段で説明する。

なお、図 1 に示す暗号処理手段 1 5 0 、 T S 処理手段 3 0 0 は、理解を容易にするため、別ブロックとして示してあるが、両機能を実行する 1 つのワンチップ L S I として構成してもよく、また、両機能をソフトウェア又はハードウェアを組み合わせた構成によって実現する構成としてもよい。

本発明の記録再生装置の構成例としては図 1 に示す構成の他に図 2 に示す構成が可能である。図 2 に示す記録再生装置 2 0 0 では、記録媒体 2 0 5 はドライブ装置としての記録媒体インタフェース (I / F) 2 1 0 から着脱が可能であり、この記録媒体 2 0 5 を別の記録再生装置に装着してもデータの読出し、書き込みが可能な構成としたものである。このように、記録媒体 1 9 5 が複数の記録再生装置において使用可能な構成を持つ図 2 のような記録再生装置においては記録再生装置毎に固有のデバイスキーを持つのではなく、複数の記録再生装置に共通な鍵、即ちシステム全体で共通な鍵をメモリ 1 8 0 に格納する構成とする。

[データ記録処理及びデータ再生処理]

次に、図 1 あるいは図 2 の記録再生装置における記録媒体に対するデータ記録処理及び記録媒体からのデータ再生処理について、図 3 及び図 4 のフローチャー

トを参照して説明する。外部からのデジタル信号のコンテンツを、記録媒体 195 に記録する場合においては、図 3 (A) のフローチャートに従った記録処理が行われる。即ち、デジタル信号のコンテンツ（デジタルコンテンツ）が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力 I / F 120 に供給されると、ステップ S 301 において、入出力 I / F 120 は、供給されるデジタルコンテンツを受信し、バス 110 を介して、TS 処理手段 300 に出力する。

TS 処理手段 300 は、ステップ S 302 において、トランスポートストリームを構成する各トランスポートパケットに A T S を付加したブロックデータを生成して、バス 110 を介して、暗号処理手段 150 に出力する。

暗号処理手段 150 は、ステップ S 303 において、受信したデジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス 110 を介して、ドライブ 190、あるいは記録媒体 I / F 210 に出力する。暗号化コンテンツは、ドライブ 190、あるいは記録媒体 I / F 210 を介して記録媒体 195 に記録 (S 304) され、記録処理を終了する。なお、暗号処理手段 150 における暗号処理については後段で説明する。

なお、IEEE1394シリアルバスを介して接続した装置相互間で、デジタルコンテンツを伝送するときの、デジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む 5 社によって、5 C D T C P (Five Company Digital Transmission Content Protection) (以下、適宜、D T C P という) が定められているが、この D T C P では、コピーフリーでないデジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、デジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたデジタルコンテンツ（暗号化コンテンツ）を復号するようになっている。

この D T C P に規格に基づくデータ送受信においては、データ受信側の入出力 I / F 120 は、ステップ S 301 で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、D T C P に規格に準拠して復号し、

平文のコンテンツとして、その後、暗号処理手段150に出力する。

D T C Pによるデジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたデジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたデジタルコンテンツを、そこに含まれるキーを用いて復号する。

なお、D T C Pによれば、正確には、キーの初期値と、デジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含まれる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、D T C Pについては、例えば、<http://www.dtcp.com>のURL (Uniform Resource Locator)で特定されるWebページにおいて、インフォメーションバージョン(Informational Version)の取得が可能である。

次に、外部からのアナログ信号のコンテンツを、記録媒体195に記録する場合の処理について、図3(B)のフローチャートに従って説明する。アナログ信号のコンテンツ(アナログコンテンツ)が、入出力I/F140に供給されると、入出力I/F140は、ステップS321において、そのアナログコンテンツを受信し、ステップS322に進み、内蔵するA/D、D/Aコンバータ141でA/D変換して、デジタル信号のコンテンツ(デジタルコンテンツ)とする。

このデジタルコンテンツは、MPEGコーデック130に供給され、ステップS323において、MPEGエンコード、即ちMPEG圧縮による符号化処理が実行され、バス110を介して、暗号処理手段150に供給される。

以下、ステップS324、S325、S326において、図3(A)のステップS302、S303における処理と同様の処理が行われる。即ち、TS処理手段300によるトランスポートパケットに対するATS付加、暗号処理手段150における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体195に記録して、記録処理を終了する。

次に、記録媒体 195 に記録されたコンテンツを再生して、デジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図 4 のフローに従って説明する。デジタルコンテンツとして外部に出力する処理は図 4 (A) のフローチャートに従った再生処理として実行される。即ち、まず最初に、ステップ S 401 において、ドライブ 190 又は記録媒体 I/F 210 によって、記録媒体 195 に記録された暗号化コンテンツが読み出され、バス 110 を介して、暗号処理手段 150 に出力される。

暗号処理手段 150 では、ステップ S 402 において、ドライブ 190 又は記録媒体 I/F 210 から供給される暗号化コンテンツが復号処理され、復号データがバス 110 を介して、TS 処理手段 300 に出力される。

TS 処理手段 300 は、ステップ S 403 において、トランスポートストリームを構成する各トランスポートパケットの A T S から出力タイミングを判定し、A T S に応じた制御を実行して、バス 110 を介して、入出力 I/F 120 に供給する。入出力 I/F 120 は、TS 処理手段 300 からのデジタルコンテンツを、外部に出力し、再生処理を終了する。なお、TS 処理手段 300 の処理、暗号処理手段 150 におけるデジタルコンテンツの復号処理については後述する。

なお、入出力 I/F 120 は、ステップ S 404 で、IEEE1394 シリアルバスを介してデジタルコンテンツを出力する場合には、D T C P の規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、デジタルコンテンツを暗号化して伝送する。

記録媒体 195 に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図 4 (B) のフローチャートに従った再生処理が行われる。

即ち、ステップ S 421、S 422、S 423 において、図 4 (A) のステップ S 401、S 402、S 403 における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段 150 において得られた復号されたデジタルコンテンツは、バス 110 を介して、M P E G コーデック 130 に供給される。

M P E G コーデック 130 では、ステップ S 424 において、デジタルコン

テンツがMPEGデコード、即ち伸長処理が実行され、入出力I/F140に供給される。入出力I/F140は、ステップS424において、MPEGコーデック130でMPEGデコードされたデジタルコンテンツを、内蔵するA/D、D/Aコンバータ141でD/A変換(S425)して、アナログコンテンツとする。そして、ステップS426に進み、入出力I/F140は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

[データフォーマット]

次に、図5を用いて、本発明における記録媒体上のデータフォーマットを説明する。本発明における記録媒体上のデータの読み書きの最小単位をブロック(block)という名前と呼ぶ。1ブロックは、 $192 * X$ (エックス) バイト (例えば $X = 32$) の大きさとなっている。

本発明では、MPEG2のTS (トランスポート・ストリーム) パケット (188バイト) にATSを付加して192バイトとして、それをX個集めて1ブロックのデータとしている。ATSは24乃至32ビットの着信時刻を示すデータであり、先にも説明したようにArrival Time Stamp (着信時刻スタンプ) の略である。ATSは各パケットの着信時刻に応じたランダム性のあるデータとして構成される。記録媒体のひとつのブロック (セクタ) には、ATSを付加したTS (トランスポート・ストリーム) パケットをX個記録する。本発明の構成では、トランスポートストリームを構成する各ブロックの第1番目のTSパケットに付加されたATSを用いてそのブロック (セクタ) のデータを暗号化するブロックキーを生成する。

ランダム性のあるATSを用いて暗号化用のブロックキーを生成することにより、ブロック毎に異なる固有キーが生成される。生成されたブロック固有キーを用いてブロック毎の暗号化処理を実行する。また、ATSを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

なお、図5に示すブロック・シード (Block Seed) は、ATSを含む付加情報

である。ブロック・シードは、さらにA T Sだけでなくコピー制限情報(C C I : Copy Control Information)も付加した構成としてもよい。この場合、A T SとC C Iを用いてブロックキーを生成する構成とすることができる。

なお、本発明の構成においては、D V D等の記録媒体上にデータを格納する場合、コンテンツの大部分のデータは暗号化されるが、図5の最下段に示すように、ブロックの先頭の m （例えば、 $m = 8$ 又は 16 ）バイトは暗号化されずに平文(Unencrypted data)のまま記録され、残りのデータ($m + 1$ バイト以降)が暗号化される。これは暗号処理が8バイト単位としての処理であるために暗号処理データ長(Encrypted data)に制約が発生するためである。なお、もし暗号処理が8バイト単位でなく、例えば1バイト単位で行えるなら、 $m = 4$ として、ブロックシード以外の部分をすべて暗号化してもよい。

[T S 処理手段における処理]

ここで、A T Sの機能について詳細に説明する。A T Sは、先にも説明したように入力トランスポートストリーム中の各トランスポートパケットの出現タイミングを保存するために付加する着信時刻スタンプである。

即ち、例えば複数のT Vプログラム(コンテンツ)が多重化されたトランスポートストリームの中から1つ又は幾つかのT Vプログラム(コンテンツ)を取り出した時、その取り出したトランスポートストリームを構成するトランスポートパケットは、不規則な間隔で現れる(図7(A)参照)。トランスポートストリームは、各トランスポートパケットの出現タイミングに重要な意味があり、このタイミングはM P E G 2システムズ(ISO/IEC 13818-1)で規定されている仮想的なデコーダであるT - S T D(Transport stream System Target Decoder)を破綻させないように符号化時に決定される。

トランスポートストリームの再生時には、各トランスポートパケットに付加されたA T Sによって出現タイミングが制御される。従って、記録媒体にトランスポートパケットを記録する場合には、トランスポートパケットの入力タイミングを保存する必要があり、トランスポートパケットをD V D等の記録媒体に記録する時に、各トランスポートパケットの入力タイミングを表すA T Sを付加して記録する。

図6に、デジタルインタフェース経由で入力されるトランスポートストリームをDVD等の記録媒体であるストレージメディアに記録する時のTS処理手段300において実行する処理を説明するブロック図を示す。端子600からは、デジタル放送等のデジタルデータとしてトランスポートストリームが入力される。図1又は図2においては、入出力I/F120を介して、あるいは入出力I/F140、MPEGコーデック130を介して端子600からトランスポートストリームが入力される。

トランスポートストリームは、ビットストリームパーサ(parser)602に入力される。ビットストリームパーサ602は、入力トランスポートストリームの中からPCR(Program Clock Reference)パケットを検出する。ここで、PCRパケットとは、MPEG2システムズで規定されているPCRが符号化されているパケットである。PCRパケットは、100msec以内の時間間隔で符号化されている。PCRは、トランスポートパケットが受信側に到着する時刻を27MHzの精度で表す。

そして、27MHzPLL603において、記録再生器が持つ27MHzクロックをトランスポートストリームのPCRにロック(Lock)させる。タイムスタンプ発生回路604は、27MHzクロックのクロックのカウント値に基づいたタイムスタンプを発生する。そして、ブロック・シード(Block seed)付加回路605は、トランスポートパケットの第1バイト目がスミージングバッファ606へ入力される時のタイムスタンプをATSとして、そのトランスポートパケットに付加する。

ATSが付加されたトランスポートパケットは、スミージングバッファ606を通過して、端子607から、暗号処理手段150に出力され、後段で説明する暗号処理が実行された後、ドライブ190(図1)、記録媒体I/F210(図2)を介してストレージメディアである記録媒体195に記録される。

図7は、入力トランスポートストリームが記録媒体に記録される時の処理の例を示す。図7(A)は、ある特定プログラム(コンテンツ)を構成するトランスポートパケットの入力を示す。ここで横軸は、ストリーム上の時刻を示す時間軸である。この例ではトランスポートパケットの入力は、図7(A)に示すように

不規則なタイミングで現れる。

図7 (B) は、ブロック・シード (Block Seed) 付加回路605の出力を示す。ブロック・シード (Block Seed) 付加回路605は、トランスポートパケット毎に、そのパケットのストリーム上の時刻を示すA T Sを含むブロック・シード (Block Seed) を付加して、ソースパケットを出力する。図7 (C) は記録媒体に記録されたソースパケットを示す。ソースパケットは、図7 (C) に示すように間隔を詰めて記録媒体に記録される。このように間隔を詰めて記録することにより記録媒体の記録領域を有効に使用できる。

図8は、記録媒体195に記録されたトランスポートストリームを再生する場合のT S処理手段300の処理構成ブロック図を示している。端子800からは、後段で説明する暗号処理手段において復号されたA T S付きのトランスポートパケットが、ブロック・シード (Block seed) 分離回路801へ入力され、A T Sとトランスポートパケットが分離される。タイミング発生回路804は、再生器が持つ27MHzクロック805のクロックカウンタ値に基づいた時間を計算する。

なお、再生の開始時において、一番最初のA T Sが初期値として、タイミング発生回路804にセットされる。比較器803は、A T Sとタイミング発生回路804から入力される現在の時刻を比較する。そして、タイミング発生回路804が発生する時間とA T Sが等しくなった時、出力制御回路802は、そのトランスポートパケットをM P E Gコーデック130又はデジタル入出力I / F 120へ出力する。

図9は、入力A V信号を記録再生器100のM P E Gコーデック130においてM P E Gエンコードして、さらにT S処理手段300においてトランスポートストリームを符号化する構成を示す。従って図9は、図1又は、図2におけるM P E Gコーデック130とT S処理手段300の両処理構成を併せて示すブロック図である。端子901からは、ビデオ信号が入力されており、それはM P E Gビデオエンコーダ902へ入力される。

M P E Gビデオエンコーダ902は、入力ビデオ信号をM P E Gビデオストリームに符号化し、それをバッファビデオストリームバッファ903へ出力する。

また、MPEGビデオエンコーダ902は、MPEGビデオストリームについてのアクセスユニット情報を多重化スケジューラ908へ出力する。ビデオストリームのアクセスユニットとは、ピクチャであり、アクセスユニット情報とは、各ピクチャのピクチャタイプ、符号化ビット量、デコードタイムスタンプである。ここで、ピクチャタイプは、I/P/Bピクチャ (picture) の情報である。また、デコードタイムスタンプは、MPEG2システムズで規定されている情報である。

端子904からは、オーディオ信号が入力されており、それはMPEGオーディオエンコーダ905へ入力される。MPEGオーディオエンコーダ905は、入力オーディオ信号をMPEGオーディオストリームに符号化し、それをバッファ906へ出力する。また、MPEGオーディオエンコーダ905は、MPEGオーディオストリームについてのアクセスユニット情報を多重化スケジューラ908へ出力する。オーディオストリームのアクセスユニットとは、オーディオフレームであり、アクセスユニット情報とは、各オーディオフレームの符号化ビット量、デコードタイムスタンプである。

多重化スケジューラ908には、ビデオとオーディオのアクセスユニット情報が入力される。多重化スケジューラ908は、アクセスユニット情報に基づいて、ビデオストリームとオーディオストリームをトランスポートパケットに符号化する方法を制御する。多重化スケジューラ908は、内部に27MHz精度の基準時刻を発生するクロックを持ち、そして、MPEG2で規定されている仮想的なデコーダモデルであるT-S TDを満たすようにして、トランスポートパケットのパケット符号化制御情報を決定する。パケット符号化制御情報は、パケット化するストリームの種類とストリームの長さである。

パケット符号化制御情報がビデオパケットの場合、スイッチ976はa側になり、ビデオストリームバッファ903からパケット符号化制御情報により指示されたペイロードデータ長のビデオデータが読み出され、トランスポートパケット符号化器909へ入力される。

パケット符号化制御情報がオーディオパケットの場合、スイッチ976はb側になり、オーディオストリームバッファ906から指示されたペイロードデータ長のオーディオデータが読み出され、トランスポートパケット符号化器909へ

入力される。

パケット符号化制御情報がPCRパケットの場合、トランスポートパケット符号化器909は、多重化スケジューラ908から入力されるPCRを取り込み、PCRパケットを出力する。パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケット符号化器909へは何も入力されない。

トランスポートパケット符号化器909は、パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケットを出力しない。それ以外の場合、パケット符号化制御情報に基づいてトランスポートパケットを生成し、出力する。従って、トランスポートパケット符号化器909は、間欠的にトランスポートパケットを出力する。到着 (Arrival) タイムスタンプ (time stamp) 計算手段910は、多重化スケジューラ908から入力されるPCRに基づいて、トランスポートパケットの第1バイト目が受信側に到着する時刻を示すATSを計算する。

多重化スケジューラ908から入力されるPCRは、MPEG2で規定されるトランスポートパケットの10バイト目の受信側への到着時刻を示すので、ATSの値は、PCRの時刻から10バイト前のバイトが到着する時刻となる。

ブロック・シード (Block Seed) 付加回路911は、トランスポートパケット符号化器909から出力されるトランスポートパケットにATSを付加する。ブロック・シード (Block seed) 付加回路911から出力されるATS付きのトランスポートパケットは、スムージングバッファ912を通して、暗号処理手段150へ入力され、後段で説明する暗号処理が実行された後、ストレージメディアである記録媒体195へ格納される。

記録媒体195へ格納されるATS付きのトランスポートパケットは、暗号処理手段150で暗号化される前に図7(C)に示すように間隔を詰めた状態で入力され、その後、記録媒体195に格納される。トランスポートパケットが間隔を詰めて記録されても、ATSを参照することによって、そのトランスポートパケットの受信側への入力時刻を制御することができる。

ところで、ATSの大きさは32ビットに決まっているわけではなく、24ビ

ット乃至31ビットでも構わない。ATSのビット長が長いほど、ATSの時間カウンタが一周する周期が長くなる。例えば、ATSが27MHz精度のバイナリカウンタである場合、24-bit長のATSが一周する時間は、約0.6秒である。この時間間隔は、一般のトランスポートストリームでは十分な大きさである。なぜなら、トランスポートストリームのパケット間隔は、MPEG2の規定により、最大0.1秒と決められているからである。しかしながら、十分な余裕を見て、ATSを24-bit以上にしてもよい。

このように、ATSのビット長を様々な長さとした場合、ブロックデータの付加データであるブロックシードの構成としていくつかの構成が可能となる。ブロック・シードの構成例を図10に示す。図10の例1は、ATSを32ビット分使用する例である。図10の例2は、ATSを30ビットとし、コピー制御情報(CCI)を2ビット分使用する例である。コピー制御情報は、それが付加されたデータのコピー制御の状態を表す情報であり、SCMS: Serial Copy Management SystemやCGMS: Copy Generation Management Systemが有名である。これらのコピー制御情報では、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー(Copy Free)、1世代のみのコピーを許可する1世代コピー許可(One Generation Copy Allowed)、コピーを認めないコピー禁止(Copy Prohibited)などの情報が表せる。

図10に示す例3は、ATSを24ビットとし、CCIを2ビット使用し、さらに他の情報を6ビット使用する例である。他の情報としては、例えばこのデータがアナログ出力される際に、アナログ映像データのコピー制御機構であるマクロビジョン(Macrovision)のオン/オフ(On/Off)を示す情報など、様々な情報を利用することが可能である。

[記録データの互換性が必要なシステムにおけるデータ記録処理に伴う暗号処理]

次に、記録データの互換性が必要なシステム、即ち、ある記録再生器において記録した記録媒体を他の記録再生器において再生可能とすることが要請されるシステムでのデータ記録処理に伴う暗号処理について説明する。記録データの互換性が必要なシステムは例えば図2に示すような記録再生装置200であり、記録

媒体 1 9 5 が他の記録再生器においても使用可能とする要請があるものである。

このようなシステムにおけるデータ記録処理における暗号化処理について、図 1 1、図 1 2 の処理ブロック図及び図 1 3 のフローチャートを用いて説明する。ここでは、記録媒体として光ディスクを例とする。この実施例は、特開平 1 1 - 2 2 4 4 6 1 号公報（特願平 1 0 - 2 5 3 1 0 号）に記載した構成と同様に、ある記録再生装置で記録したデータを、別の記録再生装置で再生できることが必要な、即ち記録データの互換性が必要なシステムである。そして、記録媒体上のデータの bit-by-bit コピーを防ぐために、記録媒体固有の識別情報としてのディスク ID (Disc ID) を、データを暗号化する鍵に作用させるようにしている。

図 1 1、図 1 2 の処理ブロック図に従って、暗号処理手段 1 5 0 が実行するデータの暗号化処理の概要について説明する。

記録再生装置 1 1 0 0 は自身のメモリ 1 8 0（図 2 参照）に格納しているマスターキー 1 1 0 1 を読み出す。マスターキー 1 1 0 1 は、ライセンスを受けた記録再生装置に格納された秘密キーであり、複数の記録再生装置に共通なキー、即ちシステム全体で共通なキーである。記録再生装置 1 1 0 0 は例えば光ディスクである記録媒体 1 1 2 0 に識別情報としてのディスク ID (Disc ID) 1 1 0 3 が既に記録されているかどうかを検査する。記録されていれば、ディスク ID (Disc ID) 1 1 0 3 を読み出し（図 1 1 に相当）、記録されていなければ、暗号処理手段 1 5 0 においてランダムに、もしくは予め定められた例えば乱数発生等の方法でディスク ID (Disc ID) 1 2 0 1 を生成し、ディスクに記録する（図 1 2 に相当）。ディスク ID (Disc ID) 1 1 0 3 はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

記録再生器 1 1 0 0 は、次にマスターキーとディスク ID を用いて、ディスク固有キー (Disc Unique Key) を生成 1 1 0 2 する。ディスク固有キー (Disc Unique Key) の具体的な生成方法としては、例えば、FIPS 180-1 で定められているハッシュ関数 SHA-1 に、マスターキーとディスク ID (Disc ID) とのビット連結により生成されるデータを入力し、その 1 6 0 ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用方法や、ブロック暗号関数を用いたハッシュ関数にマスターキー (Master Key) とディスク ID (Di

sc ID) を入力して得られた結果を用いるなどの方法が挙げられる。

次に、記録毎の固有鍵であるタイトルキー (Title Key) を暗号処理手段 150 においてランダムに、もしくは予め定められた例えば乱数発生等の方法で生成 1104し、ディスク 1120に記録する。ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキーを格納することができる。

次にディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) から、タイトル固有キー (Title Unique Key) を生成する。この生成の具体的な方法も、上記のように、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法など、幾つ挙げることができる。

なお、上記の説明では、マスターキー (Master Key) とディスク ID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてマスターキー (Master Key) とディスク ID (Disc ID) とタイトルキー (Title Key) から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、マスターキー (Master Key) とディスク ID (Disc ID) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

ところで、例えば上記の 5CDTCPに規定される伝送フォーマットのひとつを使用した場合、データはMP EG 2のTSパケットで伝送される場合がある。例えば、衛星放送を受信したセットトップボックス (STB: Set Top Box) がこの放送を記録機に 5CDTCPを用いて伝送する際に、STBは衛星放送通信路で伝送されたMP EG 2 TSパケットをIEEE1394上も伝送することが、データ変換の必要がなく望ましい。

記録再生装置 1100は記録すべきコンテンツデータをこのTSパケットの形で受信し、前述したTS処理手段300において、各TSパケットを受信した時刻情報であるATSを付加する。なお、先に説明したように、ブロックデータに付加されるブロック・シードは、ATSとコピー制御情報、さらに他の情報を組み合わせた値から構成してもよい。

A T Sを付加したT SパケットをX個（例えば $X=32$ ）並べて、1ブロックのブロックデータが形成（図5の上の図参照）され、図11、12の下段に示すように、被暗号化データとして入力されるブロックデータの先頭の第1～4バイトが分離され（セクタ1108）て出力される32ビットのA T Sを含むブロックシード（Block Seed）と、先に生成したタイトル固有キー（Title Unique Key）とから、そのブロックのデータを暗号化する鍵であるブロック・キー（Block Key）が生成1107される。

ブロック・キー（Block Key）の生成方法の例を図14に示す。図14では、いずれも32ビットのブロック・シード（Block Seed）と、64ビットのタイトル固有キー（Title Unique Key）とから、64ビットのブロックキー（Block Key）を生成する例を2つ示している。

上段に示す例1は、鍵長64ビット、入出力がそれぞれ64ビットの暗号関数を使用している。タイトル固有キー（Title Unique Key）をこの暗号関数の鍵とし、ブロックシード（Block Seed）と32ビットの定数（コンスタント）を連結した値を入力して暗号化した結果をブロックキー（Block Key）としている。

例2は、FIPS 180-1のハッシュ関数SHA-1を用いた例である。タイトル固有キー（Title Unique Key）とブロックシード（Block Seed）を連結した値をSHA-1に入力し、その160ビットの出力を、例えば下位64ビットのみ使用するなど、64ビットに縮約したものをブロックキー（Block Key）としている。

なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、例えば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロック毎にマスターキー（Master Key）とディスクID（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）を用いてブロックキー（Block Key）を生成してもよい。

ブロックキーが生成されると、生成されたブロックキー（Block Key）を用いてブロックデータを暗号化する。図11、12の下段に示すように、ブロックシード（Block Seed）を含むブロックデータの先頭の第1～mバイト（例えば $m=8$ バイト）は分離（セクタ1108）されて暗号化対象とせず、 $m+1$ バイト目

から最終データまでを暗号化 1 1 0 9 する。なお、暗号化されない m バイト中にはブロック・シードとしての第 1 ～ 4 バイトも含まれる。セクタ 1 1 0 8 により分離された第 $m + 1$ バイト以降のブロックデータは、暗号処理手段 1 5 0 に予め設定された暗号化アルゴリズムに従って暗号化 1 1 0 9 される。暗号化アルゴリズムとしては、例えば FIPS 46-2 で規定される DES (Data Encryption Standard) を用いることができる。

ここで、使用する暗号アルゴリズムのブロック長 (入出力データサイズ) が DES のように 8 バイトであるときは、 X を例えば 3 2 とし、 m を例えば 8 の倍数とすることで、端数なく $m + 1$ バイト目以降のブロックデータ全体が暗号化できる。

即ち、1 ブロックに格納する TS パケットの個数を X 個とし、暗号アルゴリズムの入出力データサイズを L バイトとし、 n を任意の自然数とした場合、 $1 9 2 * X = m + n * L$ が成り立つように X 、 m 、 L を定めることにより、端数処理が不要となる。

暗号化した第 $m + 1$ バイト以降のブロックデータは暗号処理のされていない第 1 ～ m バイトデータとともにセクタ 1 1 1 0 により結合されて暗号化コンテンツ 1 1 1 2 として記録媒体 1 1 2 0 に格納される。

以上の処理により、コンテンツはブロック単位で ATS を含むブロック・シードに基づいて生成されるブロック鍵で暗号化が施されて記録媒体に格納されることになる。先にも説明したように ATS はブロック固有のランダム性の高いデータであるので、各ブロックに設定された ATS に基づくブロック鍵は、それぞれが異なった鍵となる。即ち、ブロック毎に暗号鍵が変更され、このため暗号解析に対する強度を高めることができる。また、ブロック・シードを暗号鍵生成データとして使用することにより、ブロック毎の暗号鍵をデータと別に保存しておく必要がなく、そのため暗号鍵の保存領域が不要となり記憶領域を節約できる。また、ブロック・シードはコンテンツデータとともに書き込み読み出しが実行されるデータであるので、従来のように暗号鍵を別領域に保存する構成とは異なり、記録再生時に暗号鍵データを書き込んだり読み出したりする処理が省略でき効率的な処理が可能となる。

次に図13に示すフローチャートに従って、データ記録処理に伴って実行されるTS処理手段300におけるATS付加処理及び暗号処理手段150における暗号処理の流れを説明する。図13のS1301において、記録再生装置は自身のメモリ180に格納しているマスターキーを読み出す。

S1302において、記録媒体に識別情報としてのディスクID (Disc ID) が既に記録されているかどうかを検査する。記録されていればS1303でこのディスクIDを読み出し、記録されていなければS1304で、ランダムに、もしくは予め定められた方法でディスクIDを生成し、ディスクに記録する。次に、S1305では、マスターキーとディスクIDを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用することで求める。

次にS1306に進み、その一回の記録毎の固有の鍵としてタイトルキー (Title Key) を生成しディスクに記録する。次にS1307で、上記のディスク固有キーとタイトルキーから、タイトル固有キーを生成する。キー生成には、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法を適用する。

S1308では、記録再生装置は記録すべきコンテンツデータの被暗号化データをTSパケットの形で受信する。S1309で、TS処理手段300は、各TSパケットを受信した時刻情報であるATSを付加する。あるいはコピー制御情報CCIとATS、さらに他の情報を組み合わせた値を付加する。次に、S1310で、ATSを付加したTSパケットを順次受信し、1ブロックを形成する例えば $X=32$ に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップS1311に進み、 X 個、あるいはパケット終了までのパケットを並べて、1ブロックのブロックデータを形成する。

次に、暗号処理手段150は、S1312で、ブロックデータの先頭の32ビット (ATSを含むブロック・シード) とS1307で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

S1313では、ブロックキーを用いてS1311で形成したブロックデータ

を暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータの $m+1$ バイト目から最終データまでである。暗号化アルゴリズムは、例えばFIPS 46-2で規定されるDES (Data Encryption Standard) が適用される。

S 1 3 1 4で、暗号化したブロックデータを記録媒体に記録する。S 1 3 1 5で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければS 1 3 0 8に戻って残りのデータの処理を実行する。

[記録データの互換性が必要なシステムにおけるデータ再生処理に伴う暗号処理]

次に、上記のようにして記録媒体に記録された暗号化コンテンツを復号して再生する処理について図 1 5 の処理ブロック図と、図 1 6 のフローチャートを用いて説明する。

まず、図 1 5 に示す処理ブロック図に従って説明する。記録再生装置 1 5 0 0 はディスク 1 5 2 0 からディスクID 1 5 0 2 を、また自身のメモリからマスターキー 1 5 0 1 を読み出す。先の記録処理の説明から明らかなように、ディスクIDはディスクに記録されているか、記録されていない場合は記録再生器において生成してディスクに記録したディスク固有の識別子である。マスターキー 1 5 0 1 は、ライセンスを受けた記録再生装置に格納された秘密キーである。

記録再生装置 1 5 0 0 は、次に、ディスクID (Disc ID) とマスターキー (Master Key) を用いてディスク固有キー (Disc Unique Key) を生成 1 5 0 3 する。このキー生成方法は、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用方法や、ブロック暗号関数を用いたハッシュ関数にマスターキー (Master Key) とディスクID (Disc ID) を入力して得られた結果を用いるなどの方法が挙げられる。

次に、ディスクから読み出すべきデータに対応して記録されたタイトルキー (Title Key) 1 5 0 4 を読み出し、タイトルキー (Title Key) 1 5 0 4 とディスク固有キー (Disc Unique Key) からタイトル固有キー (Title Unique Key) を

生成 1 5 0 5 する。この生成方法も、ハッシュ関数 SHA-1、ブロック暗号関数を用いたハッシュ関数の適用が可能である。

なお、上記の説明では、マスターキー (Master Key) とディスク ID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてマスターキー (Master Key) とディスク ID (Disc ID) とタイトルキー (Title Key) から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、マスターキー (Master Key) とディスク ID (Disc ID) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

次にディスクに格納されている暗号化コンテンツ 1 5 0 7 から順次ブロックデータ (Block Data) を読み出し、ブロックデータ (Block Data) の先頭の 4 バイトを構成するブロック・シード (Block Seed) をセクタ 1 5 0 8 において分離して、タイトル固有キー (Title Unique Key) との相互処理により、ブロックキー (Block Key) を生成する。

ブロック・キー (Block Key) の生成方法は、先に説明した図 1 4 の構成を適用することができる。即ち、32 ビットのブロック・シード (Block Seed) と、64 ビットのタイトル固有キー (Title Unique Key) とから、64 ビットのブロックキー (Block Key) を生成する構成が適用できる。

なお、上記ではディスク固有キー (Disc Unique key)、タイトル固有キー (Title Unique Key)、ブロックキー (Block Key) をそれぞれ生成する例を説明したが、例えば、ディスク固有キー (Disc Unique Key) とタイトル固有キー (Title Unique Key) の生成を実行することなく、ブロック毎にマスターキー (Master Key) とディスク ID (Disc ID) とタイトルキー (Title Key) とブロックシード (Block Seed) を用いてブロックキー (Block Key) を生成してもよい。

ブロックキーが生成されると、ブロックキー (Block Key) を用いて暗号化されているブロックデータを復号 1 5 0 9 し、セクタ 1 5 1 0 を介して復号データとして出力する。なお、復号データには、トランスポートストリームを構成する各トランスポートパケットに A T S が付加されており、先に説明した T S 処理手

段 300 において、A T S に基づくストリーム処理が実行される。その後、データは、使用、例えば、画像を表示したり、音楽を鳴らしたりすることが可能となる。

このように、ブロック単位で暗号化され記録媒体に格納された暗号化コンテンツはブロック単位で A T S を含むブロック・シードに基づいて生成されるブロック鍵で復号処理が施されて再生が可能となる。

次に図 16 に示すフローチャートに従って、復号処理及び再生処理について、処理の流れを説明する。図 16 の S 1 6 0 1 において、記録再生装置はディスクからディスク I D を、また自身のメモリからマスターキーを読み出す。S 1 6 0 2 で、ディスク I D とマスターキーを用いてディスク固有キーを生成する。

次に S 1 6 0 3 で、ディスクから読み出すべきデータのタイトルキーを読み出し、S 1 6 0 4 で、タイトルキーとディスク固有キーからタイトル固有キーを生成する。次に S 1 6 0 5 でディスクから暗号化されて格納されているブロックデータを読み出す。S 1 6 0 6 で、ブロックデータの先頭の 4 バイトのブロックシード (Block Seed) と、S 1 6 0 4 で生成したタイトル固有キーを用いてブロックキーを生成する。

次に、S 1 6 0 7 で、ブロックキーを用いて暗号化されているブロックデータを復号し、S 1 6 0 8 で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければ S 1 6 0 5 に戻り残りのデータを読み出す。

〔記録されたデータの互換性が不要ないシステムにおけるデータ記録処理に伴う暗号処理〕

次に、記録データの互換性が不要ないシステム、即ち、ある記録再生器において記録した記録媒体を他の記録再生器において再生可能とすることが要請されないシステム、即ち、記録データはそれを記録した装置でのみ読み出しができればよいシステムでのデータ記録処理に伴う暗号処理について図 17 の処理ブロック図及び図 18 のフローチャートを用いて説明する。

図 17 の処理ブロック図を参照しながら、図 18 のフローチャートの処理手順に従って順次説明する。

まず、図 18 の S 1 8 0 1 において、記録再生装置 1 7 0 0 (図 17 参照) は、

その装置固有の鍵であるデバイス固有キー (Device Unique Key) を生成する。

図 17 に示すようにデバイス固有キー (Device Unique Key) の生成は L S I キー、デバイスキー、メディアキー、ドライブキーのいずれか、又はこれらの任意の組合わせデータに基づいて生成する。L S I キーは、暗号処理手段 150 (図 1 参照) を構成する L S I に対して L S I の製造時に格納されたキーである。デバイス・キーは記録再生器の製造時にフラッシュメモリ、E E P R O M 等の記憶素子に格納されたデバイス即ち記録再生器に対応して設定されたキーである。メディアキーはコンテンツを格納する記録媒体に対して設定され記録媒体に格納されたキーである。ドライブキーは、D V D ドライブ等、記録媒体のドライブ装置に対して付与されたキーである。

本実施例では、デバイス固有キー (Device Unique Key) を、L S I キー、デバイスキー、メディアキー、ドライブキーのいずれか、又はこれらの任意の組合わせデータに基づいて生成する。

例えば、L S I キーとデバイスキーを使用したデバイス固有キーの生成処理について図 19 を用いて説明する。図 19 は、例えば図 1 の暗号処理手段 150 を L S I として構成した暗号処理手段 L S I 1900 における処理例を示している。

L S I キー記憶部 1901 は、複数の暗号処理手段 L S I に共通 (従って、複数の記録再生装置にも共通) の L S I キーを記憶している。具体的には例えば、L S I 製造時のロット毎に一律のキーが格納される。また、すべての暗号処理手段 L S I に共通の L S I キーを記憶する構成としてもよいし、幾つかの暗号処理手段 L S I のグループ毎に共通の L S I キーを記憶するようにしてもよい。L S I キーを、幾つの暗号処理手段 L S I に共通とするかは、例えば、暗号処理手段 L S I の製造コストとの関係で決めることができる。

暗号処理手段 L S I 1900 の鍵生成部は、キー記憶部 1901 に記憶されている L S I キーを読み出すとともに、暗号処理手段 L S I 1900 の外部の記憶素子としての例えば記録再生装置の R O M に記憶されているデバイスキー 1910 を、バスを介して読み出すことで取得し、この L S I キー及びデバイスキーに対して、キーを生成するための関数 (鍵生成関数) を適用して、デバイス固有キー (Device Unique Key) を生成する。

なお、鍵生成関数としては、L S I キー及びデバイスキーから、デバイス固有キー (Device Unique Key) を計算することは容易であるが、その逆に、デバイス固有キー (Device Unique Key) から、L S I キーやデバイスキーを計算することはできない一方向性関数を用いることができる。具体的には、デバイス固有キー生成部 1 9 0 2 は、例えば、FIPS180-1のSHA-1ハッシュ関数等の一方向性関数に対して、L S I キーとデバイスキーとを連結したものを入力として与えて、そのハッシュ関数を演算することにより、デバイス固有キー (Device Unique Key) を生成する。デバイス固有キー (Device Unique Key) は、例えば、FIPS46-2, FIPS46-3のDES, Triple-DES等を利用した一方向性関数を用い、L S I キーで、デバイスキーを暗号化することにより求めてもよい。

このようにして得られたデバイス固有キー (Device Unique Key) と、コンテンツデータの付加データとして設定されたブロック・シードとによりブロックキーを生成して、生成したブロックキーに基づいて暗号化処理又は復号処理を実行して暗号化コンテンツ 1 9 0 6 の記録媒体 1 9 2 0 に対する格納処理、あるいは暗号化コンテンツ 1 9 0 6 の記録媒体 1 9 2 0 からの再生処理を実行する。

コンテンツを暗号化方式、及び復号方式としては、例えば、FIPS46-2に挙げられているデータ・エンクリプション・スタンダード (Data Encryption Standard) その他を用いることが可能である。

図 1 9 は、L S I キー及びデバイスキーから、デバイス固有キー (Device Unique Key) を生成する例であるが、例えば、記録媒体に固有の値としてのメディアキーが割り当てられている場合や、記録媒体のドライブに対する固有の値としてのドライブキーが割り当てられている場合には、デバイス固有キー (Device Unique Key) の生成に、そのメディアキーやドライブキーも用いることが可能である。

デバイス固有キー (Device Unique Key) を、L S I キー及びデバイスキーの他に、メディアキー及びドライブキーのすべてを用いて生成する場合の処理構成例を図 2 0 に示す。図 2 0 は、ISO/IEC9797で規定されているデータインテグリティメカニズム (D I M : Data Integrity Mechanism) によって、デバイス固有キー (Device Unique Key) を生成する処理構成例を示している。

暗号化部 2 0 0 1 は、L S I キーを、デバイスキーで暗号化し、演算器 2 0 0

4に出力する。演算器2004は、暗号化部2001の出力と、メディアキーとを排他的論理和し、暗号化部2002に供給する。暗号化部2002は、LSIキーを鍵とし、演算器2004の出力を暗号化し、演算器2005に出力する。演算器2005は、暗号化部2002の出力と、ドライブキーとを排他的論理和し、暗号化部2003に出力する。暗号化部2003は、LSIキーを鍵とし、演算器2005の出力を暗号化し、その暗号化結果を、デバイス固有キー (Device Unique Key) として出力する。

図18に戻り、データ記録処理ステップの説明を続ける。ステップS1801では、上述のようにLSIキー、デバイスキー、メディアキー、ドライブキーのいずれか、又はこれらの任意の組合わせデータに基づいてデバイス固有キーを生成する。

S1802では、記録再生装置は記録すべきコンテンツデータの被暗号化データをTSパケットの形で受信する。S1803で、TS処理手段300は、各TSパケットを受信した時刻情報であるATSを付加する。あるいはコピー制御情報CCIとATS、さらに他の情報を組み合わせた値を付加する。次に、S1804で、ATSを付加したTSパケットを順次受信し、1ブロックを形成する例えば $X=32$ に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップS1805に進み、 X 個、あるいはパケット終了までのパケットを並べて、1ブロックのブロックデータを形成する。

次に、S1806で、暗号処理手段150は、ブロックデータの先頭の32ビット (ATSを含むブロック・シード) とS1801で生成したデバイス固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

S1807では、ブロックキーを用いてS1805で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータの $m+1$ バイト目から最終データまでである。暗号化アルゴリズムは、例えばFIPS 46-2で規定されるDES (Data Encryption Standard) が適用される。

S1808で、暗号化したブロックデータを記録媒体に記録する。S1809で、全データを記録したかを判断する。全データを記録していれば、記録処理を

終了し、全データを記録していなければS 1 8 0 2に戻って残りのデータの処理を実行する。

[記録されたデータの互換性が要らないシステムにおけるデータ再生処理に伴う暗号処理]

次に、このようにして記録されたデータの再生処理について、図21の処理ブロック図及び図22のフローチャートを用いて説明する。

図21の処理ブロック図を参照しながら、図22のフローチャートの処理手順に従って順次説明する。

まず、図22のS 2 2 0 1において、記録再生装置2100（図21参照）は、その装置固有の鍵であるデバイス固有キー（Device Unique Key）を生成する。

図21に示すようにデバイス固有キー（Device Unique Key）の生成はLSIキー、デバイスキー、メディアキー、ドライブキーのいずれか、又はこれらの任意の組合わせデータに基づいて生成2101する。ここで各キーは先に説明した通り、LSIキーは、暗号処理手段150（図1、図2参照）を構成するLSIに対してLSIの製造時に格納されたキー、デバイス・キーは記録再生器の製造時にフラッシュメモリ、EEPROM等の記憶素子に格納されたデバイスに対応して設定されたキー、メディアキーはコンテンツを格納する記録媒体に対して設定され記録媒体に格納されたキー、ドライブキーは、DVDドライブ等、記録媒体のドライブ装置に対して付与されたキーである。

次にS 2 2 0 2でディスクから暗号化されて格納されているブロックデータを読み出す。S 2 2 0 3で、ブロックデータの先頭の4バイトのブロックシード（Block Seed）と、S 2 2 0 1で生成したデバイス固有キーを用いてブロックキーを生成（図21の2102）する。

次に、S 2 2 0 4で、ブロックキーを用いて暗号化されているブロックデータを復号（図21の2105）し、S 2 2 0 5で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければS 2 2 0 2に戻り残りのデータを読み出す。

なお、この処理においても記録媒体2120に格納された暗号化コンテンツ2103はブロックデータの先頭第1～4バイトのブロックシードがセクタ21

04において分離され、また暗号化されていない第1～mバイトデータは、復号処理を実行されずに、セクタ2106において結合されて出力される。復号データには、バケット毎に入力タイミングを表すATS (Arrival Time Stamp: 着信時刻スタンプ) が付加されており、前述のTS処理手段における処理により正常な再生が可能となる。

このように、本発明の構成では、ブロックデータの先頭のTSバケットの受信時刻によって変化するATSに基づいて変化するブロックキーによって、コンテンツを暗号化するようにしたので、仮に、あるコンテンツの暗号化に用いたブロックキーが漏洩しても、他のコンテンツの保護に影響はない。従来のシステムのようにひとつの暗号鍵をすべてのコンテンツの暗号化に使用した場合、コンテンツが、常に、固定のデータキーによって暗号化されるため、例えば、ある平文のコンテンツと、それを、データキーによって暗号化した暗号文のコンテンツとの組が、違法コピーを行おうとする者に入手された場合に、いわゆる線形攻撃や差分攻撃といった暗号攻撃法を用いて、データキーが解読され、これにより、そのデータキーによって暗号化した暗号化コンテンツすべてが復号され、違法にコピーされるおそれがあるが、本発明の構成では、各ブロック単位で暗号鍵が異なるため、このような自体の発生する可能性はほとんどない。

本発明の構成では、ひとつの暗号鍵で暗号化されるデータの量が1ブロックであり、極めて少ないデータ量であるため、いわゆる線形攻撃や差分攻撃といった暗号攻撃法を用いて鍵を求めることが非常に困難になる。

さらに、本発明の構成では、本来のデータの付加情報として設定されるATSに基づいて暗号鍵を生成しているので、ブロック毎に暗号鍵を変化させる構成としても、その暗号鍵を記録媒体のデータセクタのセクタヘッダ部などに新たに記録する必要がないため、余分な記録容量を消費せず、また記録、再生時にブロック毎の暗号鍵のリード、ライトなどの処理を行う必要がない。

〔記録されたデータ再生についての機器制限の設定が可能なシステムにおけるデータ暗号化及び記録処理〕

上述の構成は、マスターキーによりブロックキーを生成可能とした構成であり、共通のマスターキーを有する記録再生器においては、再生が可能となる。しかし、

ある特定のデータについては、データ記録を実行したその記録再生器でのみ再生可能としたい場合がある。以下では、このような機器制限の設定を実行する構成について説明する。

本例は、例えば先に説明した図 1、図 2 の記録再生器において記録媒体 195 が着脱可能であり、記録媒体 195 を他の記録再生器にも装着可能な構成において効果的なシステムである。即ち、記録媒体 195 に対してデータを記録したとき、その記録データを記録した記録媒体を他の記録再生器に装着した場合に再生可能とするか再生不可能とするかを設定可能としたものである。

このようなシステムにおけるデータ記録処理における暗号化処理について、図 23、図 24 の処理ブロック図及び図 25 のフローチャートを用いて説明する。ここでは、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータの bit-by-bit コピーを防ぐために、記録媒体固有の識別情報としてのディスク ID (Disc ID) を、データを暗号化する鍵に作用させるようにしている。

図 23、図 24 の処理ブロック図に従って、暗号処理手段 150 が実行するデータの暗号化処理の概要について説明する。

記録再生装置 2300 は自身のメモリ 180 (図 1, 2 参照) に格納しているマスターキー 2301、デバイス識別子としてのデバイス ID 2331、デバイス固有キー 2332 を読み出す。マスターキー 2301 は、ライセンスを受けた記録再生装置に格納された秘密キーであり、複数の記録再生装置に共通なキー、即ちシステム全体で共通なキーである。デバイス ID は記録再生装置 2300 の識別子であり、予め記録再生装置に格納されている例えば製造番号等の識別子である。このデバイス ID は公開されていてもよい。デバイス固有キーは、その記録再生器 2300 に固有の秘密鍵であり、予め個々の記録再生装置に応じて異なるように設定されて格納されたキーである。これらは予め記録再生装置 2300 のメモリに格納されている。

記録再生装置 2300 は例えば光ディスクである記録媒体 2320 に識別情報としてのディスク ID (Disc ID) 2303 が既に記録されているかどうかを検査する。記録されていれば、ディスク ID (Disc ID) 2303 を読み出し (図 23 に相当)、記録されていなければ、暗号処理手段 150 においてランダムに、も

しくは予め定められた例えば乱数発生等の方法でディスクID (Disc ID) 2401を生成し、ディスクに記録する(図24に相当)。ディスクID (Disc ID) 2303はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

記録再生器2300は、次にマスターキーとディスクIDを用いて、ディスク固有キー(Disc Unique Key)を生成2302する。ディスク固有キー(Disc Unique Key)の具体的な生成方法としては、図26に示すように、ブロック暗号関数を用いたハッシュ関数にマスターキー(Master Key)とディスクID(Disc ID)を入力して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID(Disc ID)とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー(Disc Unique Key)として使用する例2の方法が適用できる。

次に、記録毎の固有鍵であるタイトルキー(Title Key)を暗号処理手段150においてランダムに、もしくは予め定められた例えば乱数発生等の方法で生成2304し、ディスク2320に記録する。

さらに、このタイトル(データ)がデータ記録を実行した記録再生装置でのみ再生可能とする(機器制限あり)か、他の機器においても再生可能とする(再生機器制限なし)のいずれであるかを示すフラグ、即ち再生機器制限フラグ(Player Restriction Flag)を設定し2333、ディスク2320に記録する2335。さらに、機器識別情報としてのデバイスIDを取り出して2331、ディスク2320に記録する2334。

ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー2305、再生機器制限フラグ2335、デバイスID2334を格納することができる。

次にディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイスID、あるいは、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイス固有キー、いずれかの組合せから、タイトル固有キー(Title Unique Key)を生成する。

即ち、再生機器制限をしない場合には、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイス ID とからタイトル固有キー (Title Unique Key) を生成し、再生機器制限をする場合には、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイス固有キーとからタイトル固有キー (Title Unique Key) を生成する。

このタイトル固有キー (Title Unique Key) 生成の具体的な方法は、図 28 に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー (Title Key) とディスク固有キー (Disc Unique Key) と、デバイス ID (再生機器制限をしない場合) もしくはデバイス固有キー (再生機器制限をする場合) を入力して得られた結果を用いる例 1 の方法や、FIPS 180-1 で定められているハッシュ関数 SHA-1 に、マスターキーとディスク ID (Disc ID) とデバイス ID (再生機器制限をしない場合) もしくはデバイス固有キー (再生機器制限をする場合) とのビット連結により生成されるデータを入力し、その 160 ビットの出力から必要なデータ長のみをタイトル固有キー (Title Unique Key) として使用する例 2 の方法が適用できる。

なお、上記の説明では、マスターキー (Master Key) とディスク ID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) とデバイス ID、もしくはタイトルキー (Title Key) とデバイス固有キーからタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてマスターキー (Master Key) とディスク ID (Disc ID) とタイトルキー (Title Key) と、デバイス ID もしくはデバイス固有キーから直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、マスターキー (Master Key) とディスク ID (Disc ID) と、デバイス ID (再生機器制限をしない場合) もしくはデバイス固有キー (再生機器制限をする場合) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

例えば上記の 5 C D T C P に規定される伝送フォーマットのひとつを使用した場合、データは M P E G 2 の T S パケットで伝送される場合がある。例えば、衛星放送を受信したセットトップボックス (S T B : Set Top Box) がこの放送を記

録機に 5 C D T C P を用いて伝送する際に、S T B は衛星放送通信路で伝送された M P E G 2 T S パケットを IEEE1394 上も伝送することが、データ変換の必要がなく望ましい。

記録再生装置 2 3 0 0 は記録すべきコンテンツデータをこの T S パケットの形で受信し、前述した T S 処理手段 3 0 0 において、各 T S パケットを受信した時刻情報である A T S を付加する。なお、先に説明したように、ブロックデータに対する付加情報としてのブロック・シードとして A T S とコピー制御情報、さらに他の情報を組み合わせた値を付加する構成としてもよい。

A T S を付加した T S パケットを X 個（例えば $X = 32$ ）並べて、1 ブロックのブロックデータが形成（図 5 の上の図参照）され、図 2 3、2 4 の下段に示すように、被暗号化データとして入力されるブロックデータの先頭の第 1 ～ 4 バイトが分離され（セクタ 1 1 0 8）て出力される 3 2 ビットの A T S を含むブロックシード（Block Seed）と、先に生成したタイトル固有キー（Title Unique Key）とから、そのブロックのデータを暗号化する鍵であるブロック・キー（Block Key）が生成 2 3 0 7 される。ブロック・キー（Block Key）の生成方法は先に説明した図 1 4 の方法が適用可能である。

なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、例えば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロック毎にマスターキー（Master Key）とディスク ID（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）と、デバイス ID（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）を用いてブロックキー（Block Key）を生成してもよい。

ブロックキーが生成されると、生成されたブロックキー（Block Key）を用いてブロックデータを暗号化する。図 2 3、2 4 の下段に示すように、ブロックシード（Block Seed）を含むブロックデータの先頭の第 1 ～ m バイト（例えば $m = 8$ バイト）は分離（セクタ 2 3 0 8）されて暗号化対象とせず、 $m + 1$ バイト目から最終データまでを暗号化 2 3 0 9 する。なお、暗号化されない m バイト中に

はブロック・シードとしての第1～4バイトも含まれる。セクタ2308により分離された第 $m+1$ バイト以降のブロックデータは、暗号処理手段150に予め設定された暗号化アルゴリズムに従って暗号化2309される。暗号化アルゴリズムとしては、例えばFIPS 46-2で規定されるDES (Data Encryption Standard) を用いることができる。

ここで、使用する暗号アルゴリズムのブロック長（入出力データサイズ）がDESのように8バイトであるときは、 X を例えば32とし、 m を例えば8の倍数とすることで、端数なく $m+1$ バイト目以降のブロックデータ全体が暗号化できる。

即ち、1ブロックに格納するTSパケットの個数を X 個とし、暗号アルゴリズムの入出力データサイズを L バイトとし、 n を任意の自然数とした場合、 $192 * X = m + n * L$ が成り立つように X 、 m 、 L を定めることにより、端数処理が不要となる。

暗号化した第 $m+1$ バイト以降のブロックデータは暗号処理のされていない第1～ m バイトデータとともにセクタ2310により結合されて暗号化コンテンツ2312として記録媒体1120に格納される。

以上の処理により、コンテンツはブロック単位でATSを含むブロック・シードに基づいて生成されるブロック鍵で暗号化が施されて記録媒体に格納される。また、ブロック鍵は、再生機器制限をしない場合は、デバイスIDに基づいて生成され、再生機器制限をする場合は、デバイス固有キーに基づいて生成される。これらの暗号化データは、再生機器制限をした場合は、そのデータを記録した機器でのみ再生可能となる。

即ち、再生機器制限なしの場合は、ブロックデータの暗号化鍵であるブロックキーが、デバイスIDを含むデータに基づいて生成されるとともに、デバイスIDが記録媒体に格納される。従って、記録媒体を再生しようとする機器は、記録媒体からデバイスIDを取得可能であり、同様のブロックキーを生成することが可能となるのでブロックデータの復号が可能となる。しかし、再生機器制限ありの場合は、ブロックデータの暗号化鍵であるブロックキーが、デバイス固有キーを含むデータに基づいて生成される。このデバイス固有キーはデバイス毎に異なる。

る秘密鍵であり、他の機器は、そのキーを取得することはできない。また、ブロックデータを暗号化して記録媒体に格納する場合、デバイス固有キーの記録媒体に対する書き込み処理は実行されない。従って、他の再生機器では、暗号化されたブロックデータを格納した記録媒体を装着しても、同一のデバイス固有キーを取得することができないので、ブロックデータを復号するための復号キーを生成することができず、復号不可能となり再生できない。なお、再生処理の詳細については後述する。

次に図 25 に示すフローチャートに従って、データ記録処理に伴って実行される TS 処理手段 300 における ATS 付加処理及び暗号処理手段 150 における暗号処理の処理の流れを説明する。図 25 の S2501 において、記録再生装置は自身のメモリ 180 に格納しているマスターキー、デバイス識別子としてのデバイス ID、デバイス固有キーを読み出す。

S2502 において、記録媒体に識別情報としてのディスク ID (Disc ID) が既に記録されているかどうかを検査する。記録されていれば S2503 でこのディスク ID を読み出し、記録されていなければ S2504 で、ランダムに、もしくは予め定められた方法でディスク ID を生成し、ディスクに記録する。次に、S2505 では、マスターキーとディスク ID を用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1 で定められているハッシュ関数 SHA-1 を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用することで求める。

次に S2506 に進み、その一回の記録毎の固有の鍵としてのタイトルキー (Title Key)、再生機器制限フラグ (Player Restriction Flag)、さらに、機器識別情報としてのデバイス ID を取り出してディスクに記録する。次に S2507 で、上記のディスク固有キーとタイトルキーと、デバイス ID (再生機器制限をしない場合) もしくはデバイス固有キー (再生機器制限をする場合) から、タイトル固有キーを生成する。

タイトル固有キーの生成の詳細フローを図 27 に示す。暗号処理手段 150 は、ステップ S2701 において、再生機器制限をするかしないかの判定を実行する。この判定は、記録再生器を使用するユーザによって入力された指示データ、ある

いはコンテンツに付加された利用制限情報に基づいて判定する。

S 2 7 0 1 の判定が N o、即ち、再生機器制限をしない場合は、ステップ S 2 7 0 2 に進み、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイス I D とから、タイトル固有キー (Title Unique Key) を生成する。

S 2 7 0 1 の判定が Y e s、即ち、再生機器制限をする場合は、ステップ S 2 7 0 3 に進みディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイス固有キーとから、タイトル固有キー (Title Unique Key) を生成する。キー生成には、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

S 2 5 0 8 では、記録再生装置は記録すべきコンテンツデータの被暗号化データを T S パケットの形で受信する。S 2 5 0 9 で、T S 処理手段 3 0 0 は、各 T S パケットを受信した時刻情報である A T S を付加する。あるいはコピー制御情報 C C I と A T S、さらに他の情報を組み合わせた値を付加する。次に、S 2 5 1 0 で、A T S を付加した T S パケットを順次受信し、1 ブロックを形成する例えば $X = 32$ に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップ S 2 5 1 1 に進み、 X 個、あるいはパケット終了までのパケットを並べて、1 ブロックのブロックデータを形成する。

次に、暗号処理手段 1 5 0 は、S 2 5 1 2 で、ブロックデータの先頭の 32 ビット (A T S を含むブロック・シード) と S 2 5 0 7 で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

S 2 5 1 3 では、ブロックキーを用いて S 2 5 1 1 で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータの $m + 1$ バイト目から最終データまでである。暗号化アルゴリズムは、例えば FIPS 46-2 で規定される D E S (Data Encryption Standard) が適用される。

S 2 5 1 4 で、暗号化したブロックデータを記録媒体に記録する。S 2 5 1 5 で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければ S 2 5 0 8 に戻って残りのデータの処理

を実行する。

[記録されたデータ再生についての機器制限の設定が可能なシステムにおけるデータ復号及び再生処理]

次に、上記のようにして記録媒体に記録された暗号化コンテンツを復号して再生する処理について図29の処理ブロック図と、図30のフローチャートを用いて説明する。

まず、図29に示す処理ブロック図に従って説明する。記録再生装置2900はディスク2920からディスクID2902を、また自身のメモリからマスターキー2901、デバイス識別子としてのデバイスID2931、デバイス固有キー2932を読み出す。先の記録処理の説明から明らかなように、ディスクIDはディスクに記録されているか、記録されていない場合は記録再生器において生成してディスクに記録したディスク固有の識別子である。マスターキー2901は、ライセンスを受けた記録再生装置に格納された秘密キーであり、デバイスIDは記録再生装置2900固有の識別子、デバイス固有キーは、その記録再生器に固有の秘密鍵である。

記録再生装置2900は、次に、ディスクID (Disc ID) とマスターキー (Master Key) を用いてディスク固有キー (Disc Unique Key) を生成2903する。このキー生成方法は、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用方法や、ブロック暗号関数を用いたハッシュ関数にマスターキー (Master Key) とディスクID (Disc ID) を入力して得られた結果を用いるなどの方法が挙げられる。

次に、ディスクから読み出すべきデータに対応して記録されたタイトルキー (Title Key) 2905を読み出し、さらに、このデータを記録した記録再生器のデバイスID2935と、データに対応して設定された再生機器制限フラグ2934を読み出し、読み出した再生機器制限フラグ2933が示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスID2935と自己のデバイスID2931が一致する」か、あるいは、読み出した再生

機器制限フラグ 2 9 3 3 が示す再生機器制限情報が、「再生機器制限なし」である場合は、再生可能となり、読み出した再生機器制限フラグ 2 9 3 3 が示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイス ID 2 9 3 4 と自己のデバイス ID 2 9 3 1 が一致しない」場合は、再生不可能となる。

再生不可能とされる場合は、データは、そのデータを記録した記録再生器固有のデバイス固有キーに基づいて生成されたブロックキーによって暗号化されており、そのデータを記録した記録再生器以外の記録再生器は同一のデバイス固有キーを保有しないので、データを復号するためのブロックキーを生成することができない場合である。

再生可能である場合は、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイス ID、あるいは、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイス固有キー、いずれかの組合せから、タイトル固有キー (Title Unique Key) を生成する。

即ち、再生機器制限をしない設定である場合には、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイス ID とからタイトル固有キー (Title Unique Key) を生成し、再生機器制限をする設定である場合には、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、自己のデバイス固有キーとからタイトル固有キー (Title Unique Key) を生成する。このキー生成方法としては、ハッシュ関数 SHA-1、ブロック暗号関数を用いたハッシュ関数の適用が可能である。

なお、上記の説明では、マスターキー (Master Key) とディスク ID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) とデバイス ID、もしくはタイトルキー (Title Key) とデバイス固有キーからタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてマスターキー (Master Key) とディスク ID (Disc ID) とタイトルキー (Title Key) と、デバイス ID もしくはデバイス固有キーから直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、マスタ

ーキー (Master Key) とディスク I D (Disc ID) と、デバイス I D (再生機器制限をしない場合) もしくはデバイス固有キー (再生機器制限をする場合) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

次にディスクに格納されている暗号化コンテンツ 2 9 1 2 から順次ブロックデータ (Block Data) を読み出し、ブロックデータ (Block Data) の先頭の 4 バイトを構成するブロック・シード (Block Seed) をセクタ 2 9 1 0 において分離して、タイトル固有キー (Title Unique Key) との相互処理により、ブロックキー (Block Key) を生成する。

ブロック・キー (Block Key) の生成方法は、先に説明した図 1 4 の構成を適用することができる。即ち、3 2 ビットのブロック・シード (Block Seed) と、6 4 ビットのタイトル固有キー (Title Unique Key) とから、6 4 ビットのブロックキー (Block Key) を生成する構成が適用できる。

なお、上記ではディスク固有キー (Disc Unique key)、タイトル固有キー (Title Unique Key)、ブロックキー (Block Key) をそれぞれ生成する例を説明したが、例えば、ディスク固有キー (Disc Unique Key) とタイトル固有キー (Title Unique Key) の生成を実行することなく、ブロック毎にマスターキー (Master Key) とディスク I D (Disc ID) とタイトルキー (Title Key) と、ブロックシード (Block Seed) と、デバイス I D (再生機器制限をしない場合) もしくはデバイス固有キー (再生機器制限をする場合) を用いてブロックキー (Block Key) を生成してもよい。

ブロックキーが生成されると、ブロックキー (Block Key) を用いて暗号化されているブロックデータを復号 2 9 0 9 し、セクタ 2 9 0 8 を介して復号データとして出力する。なお、復号データには、トランスポートストリームを構成する各トランスポートパケットに A T S が付加されており、先に説明した T S 処理手段 3 0 0 において、A T S に基づくストリーム処理が実行される。その後、データは、使用、例えば、画像を表示したり、音楽を鳴らしたりすることが可能となる。

このように、ブロック単位で暗号化され記録媒体に格納された暗号化コンテンツはブロック単位で A T S を含むブロック・シードに基づいて生成されるブロッ

ク鍵で復号処理が施されて再生が可能となる。

次に図 30 に示すフローチャートに従って、復号処理及び再生処理について、処理の流れを説明する。図 30 の S 3001 において、記録再生装置はディスクからディスク ID を、また自身のメモリからマスターキー、デバイス ID、デバイス固有キーを読み出す。S 3002 で、ディスク ID とマスターキーを用いてディスク固有キーを生成する。

次に S 3003 で、ディスクから読み出すべきデータのタイトルキー、さらに、このデータを記録した記録再生器のデバイス ID と、データに対応して設定された再生機器制限フラグを読み出す。

次に、S 3004 で読み出すべきデータが再生可能か否かを判定する。判定の詳細を図 31 に示す。図 31 のステップ S 3101 では、読み出した再生機器制限フラグの示す再生機器制限情報が、「再生機器制限あり」の設定であるか否かを判定する。ありの場合は、ステップ S 3102 において、「記録媒体から読み出したデバイス ID と自己のデバイス ID が一致するか否か」を判定する。一致する場合は、再生可能と判定する。ステップ S 3101 において、「再生機器制限あり」の設定でないと判定された場合も、再生可能と判定する。読み出した再生機器制限フラグが示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイス ID と自己のデバイス ID が一致しない」場合は、再生不可能と判定する。

次に、S 3005 で、タイトル固有キーの生成を行う。タイトル固有キーの生成の詳細フローを図 32 に示す。暗号処理手段 150 は、ステップ S 3201 において、再生機器制限をするの設定であるか、しないの設定であるかの判定を実行する。この判定は、ディスクから読み出した再生機器制限フラグに基づいて実行される。

S 3201 の判定が No、即ち、再生機器制限をしない設定である場合は、ステップ S 3202 に進み、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイス ID とから、タイトル固有キー (Title Unique Key) を生成する。

S 3201 の判定が Yes、即ち、再生機器制限をする場合は、ステップ S 3

203に進みディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、自己の記録再生器の有するデバイス固有キーとから、タイトル固有キー (Title Unique Key) を生成する。キー生成には、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

次にS3006でディスクから暗号化されて格納されているブロックデータを読み出す。S3007で、ブロックデータの先頭の4バイトのブロックシード (Block Seed) と、S3005で生成したタイトル固有キーを用いてブロックキーを生成する。

次に、S3008で、ブロックキーを用いて暗号化されているブロックデータを復号し、S3009で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければS3006に戻り残りのデータを読み出す。

以上のように、再生機器制限をしない場合は、デバイスIDに基づいてブロックキーを生成し、再生機器制限をする場合は、デバイス固有キーに基づいてブロックキーを生成するという2つの設定が可能であり、いずれかの設定に基づいてコンテンツをブロック単位で暗号化して記録媒体に格納することができる。記録媒体に格納されたデータを再生する場合、デバイス固有キーに基づいて暗号化されたデータに関しては、そのデータを記録した機器でのみ再生可能とする構成となり、再生機器制限をしない場合は、ディスクに記録したデバイスIDを用いて他の機器がブロックキーを生成することが可能となるので他の機器における復号処理、再生処理を実行を可能とすることができる。

[記録処理におけるコピー制御]

さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしてもよいもの (コピー可能) かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録

再生を行う場合の図1又は図2の記録再生装置の処理について、図33及び図34のフローチャートを参照して説明する。

まず、外部からのデジタル信号のコンテンツを、記録媒体に記録する場合においては、図33(A)のフローチャートに従った記録処理が行われる。図33(A)の処理について説明する。図1の記録再生装置100を例として説明する。デジタル信号のコンテンツ(デジタルコンテンツ)が、例えば、IEEE1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS3301において、入出力I/F120は、そのデジタルコンテンツを受信し、ステップS3302に進む。

ステップS3302では、入出力I/F120は、受信したデジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力I/F120が受信したコンテンツが暗号化されていない場合(例えば、上述のDTCPを使用せずに、平文のコンテンツが、入出力I/F120に供給された場合)には、そのコンテンツは、コピー可能であると判定される。

また、記録再生装置100がDTCPに準拠している装置であるとし、DTCPに従って処理を実行するものとする。DTCPでは、コピーを制御するためのコピー制御情報としての2ビットのEMI(Encryption Mode Indicator)が規定されている。EMIが00B(Bは、その前の値が2進数であることを表す)である場合は、コンテンツがコピーフリーのもの(Copy-freely)であることを表し、EMIが01Bである場合には、コンテンツが、それ以上のコピーをすることができないもの(No-more-copies)であることを表す。さらに、EMIが10Bである場合は、コンテンツが、1度だけコピーして良いもの(Copy-one-generation)であることを表し、EMIが11Bである場合には、コンテンツが、コピーが禁止されているもの(Copy-never)であることを表す。

記録再生装置100の入出力I/F120に供給される信号にEMIが含まれ、そのEMIが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、EMIが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

ステップS3302において、コンテンツがコピー可能でないと判定された場

合、ステップS 3 3 0 3～S 3 3 0 5をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体1 9 5に記録されない。

また、ステップS 3 3 0 2において、コンテンツがコピー可能であると判定された場合、ステップS 3 3 0 3に進み、以下、ステップS 3 3 0 3～S 3 3 0 5において、図3 (A)のステップS 3 0 2、S 3 0 3、S 3 0 4における処理と同様の処理が行われる。即ち、TS処理手段3 0 0によるトランスポートパケットに対するATS付加、暗号処理手段I 5 0における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体1 9 5に記録して、記録処理を終了する。

なお、EMIは、入出力I/F 1 2 0に供給されるデジタル信号に含まれるものであり、デジタルコンテンツが記録される場合には、そのデジタルコンテンツとともに、EMI、あるいは、EMIと同様にコピー制御状態を表す情報（例えば、D T C Pにおけるembedded CCIなど）も記録される。

この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

本発明の記録再生装置では、このEMIやembedded CCIなどのコピー制御情報を、TSパケットに付加する形で記録する。即ち、図1 0の例2や例3のように、ATSを2 4ビット乃至3 0ビット分と、コピー制御情報を加えた3 2ビットを図5に示すように各TSパケットに付加する。

外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図3 3 (B)のフローチャートに従った記録処理が行われる。図3 3 (B)の処理について説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力I/F 1 4 0に供給されると、入出力I/F 1 4 0は、ステップS 3 3 1 1において、そのアナログコンテンツを受信し、ステップS 3 3 1 2に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

ここで、ステップS 3 3 1 2の判定処理は、例えば、入出力I/F 1 4 0で受信した信号に、マクロビジョン(Macrovision)信号や、CGMS-A(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、VHS方式のビデオカセットテープに記録すると、

ノイズとなるような信号であり、これが、入出力 I/F 140 で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

また、例えば、CGMS-A 信号は、デジタル信号のコピー制御に用いられる CGMS 信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、1 度だけコピーして良いもの(Copy-one-generation)、又はコピーが禁止されているもの(Copy-never)のうちのいずれであるかを表す。

従って、CGMS-A 信号が、入出力 I/F 140 で受信した信号に含まれ、かつ、その CGMS-A 信号が、Copy-freely や Copy-one-generation を表している場合には、アナログコンテンツは、コピー可能であると判定される。また、CGMS-A 信号が、Copy-never を表している場合には、アナログコンテンツは、コピー可能でないと判定される。

さらに、例えば、マクロビジョン信号も、CGMS-A 信号も、入出力 I/F 4 で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

ステップ S 3 3 1 2 において、アナログコンテンツがコピー可能でないと判定された場合、ステップ S 3 3 1 3 乃至 S 3 3 1 7 をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体 195 に記録されない。

また、ステップ S 3 3 1 2 において、アナログコンテンツがコピー可能であると判定された場合、ステップ S 3 3 1 3 に進み、以下、ステップ S 3 3 1 3 乃至 S 3 3 1 7 において、図 3 (B) のステップ S 3 2 2 乃至 S 3 2 6 における処理と同様の処理が行われ、これにより、コンテンツがデジタル変換、MPEG 符号化、TS 処理、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

なお、入出力 I/F 140 で受信したアナログ信号に、CGMS-A 信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、その CGMS-A 信号も、記録媒体に記録される。即ち、図 10 で示した CCI もしくはその他の情報の部分に、この信号が記録される。この際、一般的には、Copy-one-generation を表す情報は、それ以上のコピーを許さないよう、No-more-copie

sに変換されて記録される。但し、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

〔再生処理におけるコピー制御〕

次に、記録媒体に記録されたコンテンツを再生して、デジタルコンテンツとして外部に出力する場合においては、図34(A)のフローチャートに従った再生処理が行われる。図34(A)の処理について説明する。まず最初に、ステップS3401、S3402、S3403において、図4(A)のステップS401、S402、S403における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段150において復号処理がなされ、TS処理がなされる。各処理が実行されたデジタルコンテンツは、バス110を介して、入出力I/F120に供給される。

入出力I/F120は、ステップS3404において、そこに供給されるデジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力I/F120に供給されるデジタルコンテンツにEMI、あるいは、EMIと同様にコピー制御状態を表す情報（コピー制御情報）が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

また、例えば、入出力I/F120に供給されるデジタルコンテンツにEMIが含まれる場合、従って、コンテンツの記録時に、DTCFの規格に従って、EMIが記録された場合には、そのEMI（記録されたEMI(Recorded EMI)）が、Copy-freelyであるときには、デジタルコンテンツは、後でコピー可能なものであると判定される。また、EMIが、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないと判定される。

なお、一般的には、記録されたEMIが、Copy-one-generationやCopy-neverであることはない。Copy-one-generationのEMIは記録時にNo-more-copiesに変換され、また、Copy-neverのEMIを持つデジタルコンテンツは、記録媒体に記録されないからである。但し、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

ステップS 3 4 0 4において、コンテンツが、後でコピー可能なものであると判定された場合、ステップS 3 4 0 5に進み、入出力I / F 1 2 0は、そのデジタルコンテンツを、外部に出力し、再生処理を終了する。

また、ステップS 3 4 0 4において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップS 3 4 0 6に進み、入出力I / F 1 2 0は、例えば、D T C Pの規格等に従って、デジタルコンテンツを、そのデジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

即ち、例えば、上述のように、記録されたE M I が、No-more-copiesである場合（もしくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたE M I がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

このため、入出力I / F 1 2 0は、D T C Pの規格に従い、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、D T C Pの規格に準拠した装置である場合）には、デジタルコンテンツを暗号化して、外部に出力する。

次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図3 4（B）のフローチャートに従った再生処理が行われる。図3 4（B）の処理について説明する。ステップS 3 4 1 1乃至S 3 4 1 5において、図4（B）のステップS 4 2 1乃至S 4 2 5における処理と同様の処理が行われる。即ち、暗号化コンテンツの読み出し、復号処理、T S処理、M P E Gデコード、D / A変換が実行される。これにより得られるアナログコンテンツは、入出力I / F 1 4 0で受信される。

入出力I / F 1 4 0は、ステップS 3 4 1 6において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、記録されていたコンテンツとともにコピー制御情報が記録されていなかった場合には、そのコンテンツは、後でコピー可能なものであると判定される。

また、コンテンツの記録時に、例えばD T C Pの規格に従って、E M I 又はコピー制御情報が記録された場合には、そのE M I 又はコピー制御情報が、Copy-f

reelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

また、EMI又はコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI又はコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないと判定される。

さらに、例えば、入出力I/F140に供給されるアナログコンテンツにCGMS-A信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにCGMS-A信号が記録された場合には、そのCGMS-A信号が、Copy-freelyであるときには、アナログコンテンツは、後でコピー可能なものであると判定される。また、CGMS-A信号が、Copy-neverであるときには、アナログコンテンツは、後でコピー可能なものでないと判定される。

ステップS3416において、アナログコンテンツが、後でコピー可能であると判定された場合、ステップS3417に進み、入出力I/F140は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

また、ステップS3416において、アナログコンテンツが、後でコピー可能でないと判定された場合、ステップS3418に進み、入出力I/F140は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

即ち、例えば、上述のように、記録されたEMI等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

このため、入出力I/F140は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すCGMS-A信号を付加して、外部に出力する。また、例えば、記録されたCGMS-A信号が、Copy-neverである場

合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力 I/F 4 は、C G M S - A 信号を Copy-never に変更して、アナログコンテンツとともに、外部に出力する。

以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

[データ処理手段の構成]

なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段 150 は暗号化／復号 L S I として構成することも可能であるが、汎用のコンピュータや、1チップのマイクロコンピュータにプログラムを実行させることにより行う構成とする 것도可能である。同様に T S 処理手段 300 も処理をソフトウェアによって実行することが可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや1チップのマイクロコンピュータ等にインストールされる。図35は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク 3505 や R O M 3503 に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、C D - R O M (Compact Disc Read Only Memory)、M O (Magneto optical) ディスク、D V D (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体 3510 に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体 3510 は、いわゆるパッケージソフトウェアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体 3510 からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、L A N (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通

信部 3508 で受信し、内蔵するハードディスク 3505 にインストールすることができる。

コンピュータは、CPU (Central Processing Unit) 3502 を内蔵している。CPU 3502 には、バス 3501 を介して、入出力インタフェース 3511 が接続されており、CPU 3502 は、入出力インタフェース 3510 を介して、ユーザによって、キーボードやマウス等で構成される入力部 3507 が操作されることにより指令が入力されると、それに従って、ROM (Read Only Memory) 3503 に格納されているプログラムを実行する。

あるいは、CPU 3502 は、ハードディスク 3505 に格納されているプログラム、衛星もしくはネットワークから転送され、通信部 3508 で受信されてハードディスク 3505 にインストールされたプログラム、又はドライブ 3509 に装着されたリムーバブル記録媒体 3510 から読み出されてハードディスク 3505 にインストールされたプログラムを、RAM (Random Access Memory) 3504 にロードして実行する。

これにより、CPU 3502 は、上述したフローチャートに従った処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU 3502 は、その処理結果を、必要に応じて、例えば、入出力インタフェース 3511 を介して、LCD (Liquid Crystal Display) やスピーカ等で構成される出力部 3506 から出力、あるいは、通信部 3508 から送信、さらには、ハードディスク 3505 に記録させる。

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

また、プログラムは、1つのコンピュータにより処理されるものであってもよいし、複数のコンピュータによって分散処理されるものであってもよい。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであってもよい。

なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、1チップの暗号化／復号LSIで構成する例を中心として説明したが、コンテンツの

暗号化／復号を行うブロックは、例えば、図1及び図2に示すCPU170が実行する1つのソフトウェアモジュールとして実現することも可能である。同様に、TS処理手段300の処理もCPU170が実行する1つのソフトウェアモジュールとして実現することが可能である。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。即ち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

産業上の利用可能性

本発明の情報記録再生装置及び方法によれば、各パケットの着信時刻に応じたランダム性のあるデータとして構成されるATSを用いてブロック・データを暗号化するブロックキーを生成する構成としたので、ブロック毎に異なる固有キーを生成することが可能となり、ブロック毎に暗号鍵を変更でき、暗号解析に対する強度を高めることができる。また、ATSを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

請求の範囲

1. 記録媒体に情報を記録する情報記録装置において、

間欠的なトランスポートパケットからなるトランスポートストリームを構成する各パケットに受信時刻情報 (A T S) を付加するトランスポート・ストリーム処理手段と、

前記受信時刻情報 (A T S) の付加された 1 以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報 (A T S) を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理手段と、を有し、

前記暗号処理手段によって暗号化したデータを前記記録媒体に記録する構成としたことを特徴とする情報記録装置。

2. 前記暗号処理手段は、

前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報 (A T S) を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する暗号処理用のブロックキーを生成する構成であることを特徴とする請求の範囲第 1 項に記載の情報記録装置。

3. 前記暗号処理手段は、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスク I D と、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成する構成であることを特徴とする請求の範囲第 1 項に記載の情報記録装置。

4. 前記暗号処理手段は、

記録媒体固有の記録媒体識別子であるディスク I D と、前記記録媒体に記録すべきデータ固有のタイトルキーとを生成して前記記録媒体に格納する処理を実行

する構成を有することを特徴とする請求の範囲第1項に記載の情報記録装置。

5. 前記ブロックシードは、

前記受信時刻情報（A T S）の他にコピー制御情報を含むデータであることを特徴とする請求の範囲第1項に記載の情報記録装置。

6. 前記暗号処理手段は、

前記ブロックデータの暗号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより暗号化する構成であることを特徴とする請求の範囲第1項に記載の情報記録装置。

7. 前記暗号処理手段は、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする請求の範囲第1項に記載の情報記録装置。

8. 前記暗号処理手段は、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする請求の範囲第1項に記載の情報記録装置。

9. 前記暗号処理手段は、

該暗号処理手段を構成するLSIに格納されたLSIキー、前記情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する暗号処理用のブロックキーを生成する構成であることを特徴とする請求の範囲第1項に記載の情報記

録装置。

10. 前記暗号処理手段は、

前記ブロックデータに対するブロックキーによる暗号処理をDESアルゴリズムに従って実行する構成であることを特徴とする請求の範囲第1項に記載の情報記録装置。

11. 前記情報記録装置は、

記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、
前記インタフェース手段は、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする請求の範囲第1項に記載の情報記録装置。

12. 前記情報記録装置は、

記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、
前記インタフェース手段は、コピーを制御するためのコピー制御情報としての2ビットのEMI(Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする請求の範囲第1項に記載の情報記録装置。

13. 記録媒体から情報を再生する情報再生装置において、

前記記録媒体に記録された暗号データを復号する暗号処理手段であり、
複数のトランスポートパケットの各々に受信時刻情報(ATS)を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する暗号処理手段と、

前記暗号処理手段において復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報(ATS)に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段と、

を有することを特徴とする情報再生装置。

14. 前記暗号処理手段は、

前記ブロックデータを構成する複数のトランスポートバケットの先頭のトランスポートバケットに付加された受信時刻情報（A T S）を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する復号処理用のブロックキーを生成する構成であることを特徴とする請求の範囲第 1 3 項に記載の情報再生装置。

1 5 . 前記暗号処理手段は、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスク I D と、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成する構成であることを特徴とする請求の範囲第 1 3 項に記載の情報再生装置。

1 6 . 前記ブロックシードは、

前記受信時刻情報（A T S）の他にコピー制御情報を含むデータであることを特徴とする請求の範囲第 1 3 項に記載の情報再生装置。

1 7 . 前記暗号処理手段は、

前記ブロックデータの復号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより復号する構成であることを特徴とする請求の範囲第 1 3 項に記載の情報再生装置。

1 8 . 前記暗号処理手段は、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスク I D と、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする請求の範囲第 1 3 項に記載の情報再生装置。

1 9 . 前記暗号処理手段は、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスク I D と、前記記録媒体に記録すべきデータ固有のタイトルキーとに

基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする請求の範囲第13項に記載の情報再生装置。

20. 前記暗号処理手段は、

該暗号処理手段を構成するLSIに格納されたLSIキー、前記情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する復号処理用のブロックキーを生成する構成であることを特徴とする請求の範囲第13項に記載の情報再生装置。

21. 前記暗号処理手段は、

前記ブロックデータに対するブロックキーによる復号処理をDESアルゴリズムに従って実行する構成であることを特徴とする請求の範囲第13項に記載の情報再生装置。

22. 前記情報再生装置は、

記録媒体からの再生対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて再生実行の可否を制御する構成を有することを特徴とする請求の範囲第13項に記載の情報再生装置。

23. 前記情報再生装置は、

記録媒体からの再生対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、コピーを制御するためのコピー制御情報としての2ビットのEMI(Encryption Mode Indicator)を識別し、該EMIに基づいて再生実行の可否を制御する構成を有することを特徴とする請求の範囲第13項に記載の情報再生装置。

24. 記録媒体に情報を記録する情報記録方法において、

トランスポートパケットからなるトランスポートストリームを構成する各パケ

ットに受信時刻情報（A T S）を付加するトランスポート・ストリーム処理ステップと、

前記受信時刻情報（A T S）の付加された1以上のバケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報（A T S）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理ステップと、を有し、

前記暗号処理ステップによって暗号化したデータを前記記録媒体に記録することを特徴とする情報記録方法。

25. 前記暗号処理ステップは、

前記ブロックデータを構成する複数のトランスポートバケットの先頭のトランスポートバケットに付加された受信時刻情報（A T S）を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する暗号処理用のブロックキーを生成することを特徴とする請求の範囲第24項に記載の情報記録方法。

26. 前記暗号処理ステップは、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成することを特徴とする請求の範囲第24項に記載の情報記録方法。

27. 前記情報記録方法は、さらに、

記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとを生成して前記記録媒体に格納する処理を実行する識別子生成ステップを有することを特徴とする請求の範囲第24項に記載の情報記録方法。

28. 前記暗号処理ステップは、

前記ブロックデータの暗号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキー

により暗号化することを特徴とする請求の範囲第24項に記載の情報記録方法。

29. 前記暗号処理ステップは、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする請求の範囲第24項に記載の情報記録方法。

30. 前記暗号処理ステップは、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする請求の範囲第24項に記載の情報記録方法。

31. 前記暗号処理ステップは、

暗号処理手段を構成するLSIに格納されたLSIキー、情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する暗号処理用のブロックキーを生成することを特徴とする請求の範囲第24項に記載の情報記録方法。

32. 前記暗号処理ステップは、

前記ブロックデータに対するブロックキーによる暗号処理をDESアルゴリズムに従って実行することを特徴とする請求の範囲第24項に記載の情報記録方法。

33. 前記情報記録方法は、さらに、

前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御するコピー制御ステップを有することを特徴とする請求の範囲第24項に記載の情報記録方法。

34. 前記情報記録方法は、さらに、

コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体に対する記録実行の可否を制御するコピー制御ステップを有することを特徴とする請求の範囲第24項に記載の情報記録方法。

35. 記録媒体から情報を再生する情報再生方法において、

複数のトランスポートパケットの各々に受信時刻情報(ATS)を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する復号処理ステップと、

前記暗号処理ステップにおいて復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報(ATS)に基づいてデータ出力制御を実行するトランスポート・ストリーム処理ステップと、

を有することを特徴とする情報再生方法。

36. 前記復号処理ステップは、

前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する復号処理用のブロックキーを生成することを特徴とする請求の範囲第35項に記載の情報再生方法。

37. 前記復号処理ステップは、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成することを特徴とする請求の範囲第35項に記載の情報再生方法。

38. 前記復号処理ステップは、

前記ブロックデータの復号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキー

により復号することを特徴とする請求の範囲第35項に記載の情報再生方法。

39. 前記復号処理ステップは、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする請求の範囲第35項に記載の情報再生方法。

40. 前記復号処理ステップは、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする請求の範囲第35項に記載の情報再生方法。

41. 前記復号処理ステップは、

暗号処理手段を構成するLSIに格納されたLSIキー、情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する復号処理用のブロックキーを生成することを特徴とする請求の範囲第35項に記載の情報再生方法。

42. 前記復号処理ステップは、

前記ブロックデータに対するブロックキーによる復号処理をDESアルゴリズムに従って実行することを特徴とする請求の範囲第35項に記載の情報再生方法。

43. 前記情報再生方法は、さらに、

前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体からの情報再生実行の可否を制御するコピー制御ステップを有することを特徴とする請求の範囲第35項に記載の情報再生方法。

44. 前記情報再生方法は、さらに、

コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体からの情報再生実行の可否を制御するコピー制御ステップを有することを特徴とする請求の範囲第35項に記載の情報再生方法。

45. トランスポートストリームを構成する各パケットに受信時刻情報 (ATS) を付加した1以上のパケットからなるブロックデータの暗号化鍵として使用されるブロックキーの生成情報となる受信時刻情報 (ATS) を含むブロックシードを有する非暗号化データ部と、

前記ブロックキーにより暗号化された暗号化データ部と、

を構成要素とするブロックデータを記録したことを特徴とする記録媒体。

46. 記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

間欠的なトランスポートパケットからなるトランスポートストリームを構成する各パケットに受信時刻情報 (ATS) を付加するトランスポート・ストリーム処理ステップと、

前記受信時刻情報 (ATS) の付加された1以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理ステップと、

を有することを特徴とするプログラム提供媒体。

47. 記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

複数のトランスポートパケットの各々に受信時刻情報 (ATS) を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号

処理を実行する復号処理ステップと、

前記暗号処理ステップにおいて復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（A T S）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理ステップと、

を有することを特徴とするプログラム提供媒体。

THIS PAGE BLANK (USPTO)

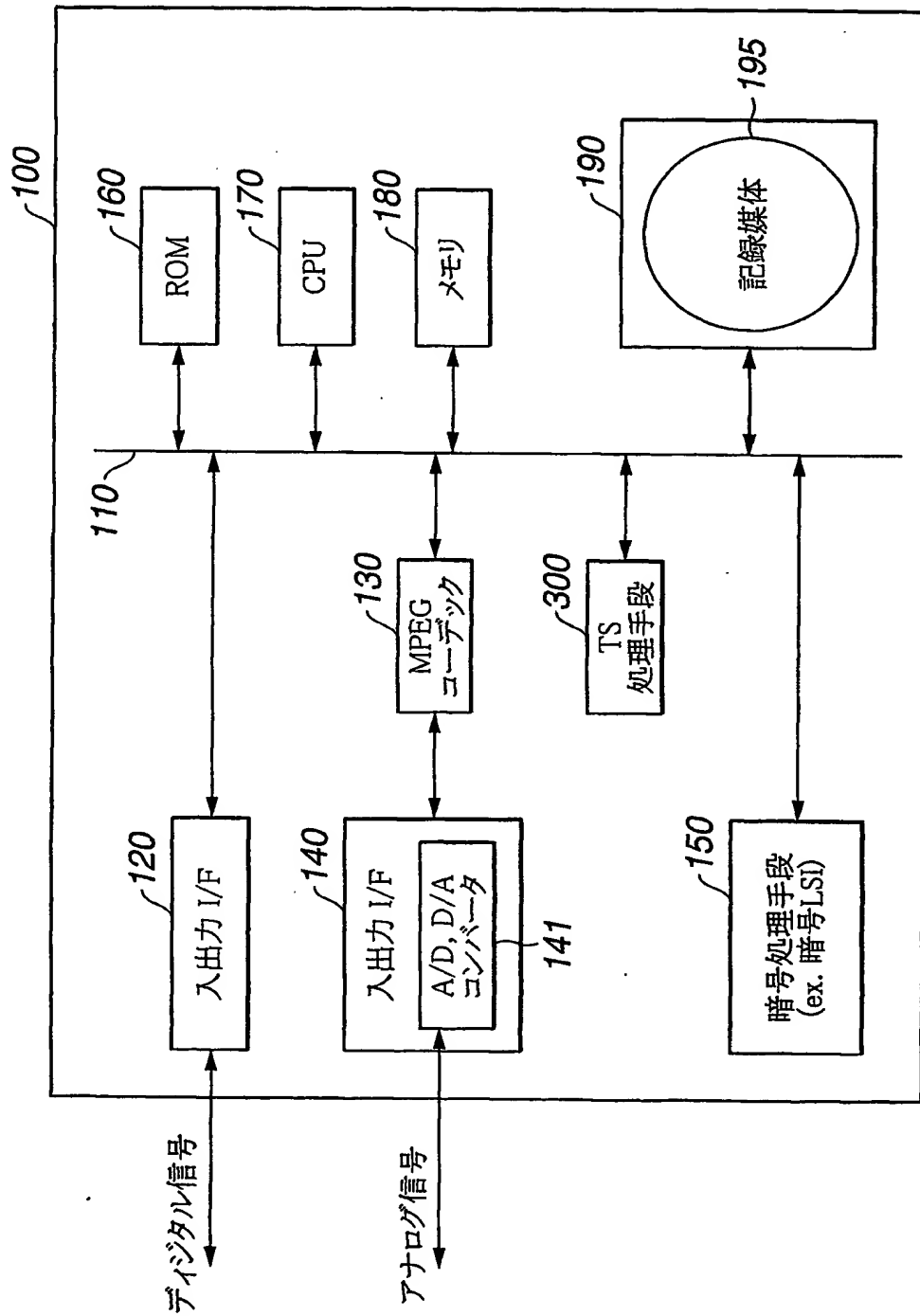


FIG.1

THIS PAGE BLANK (USPTO)

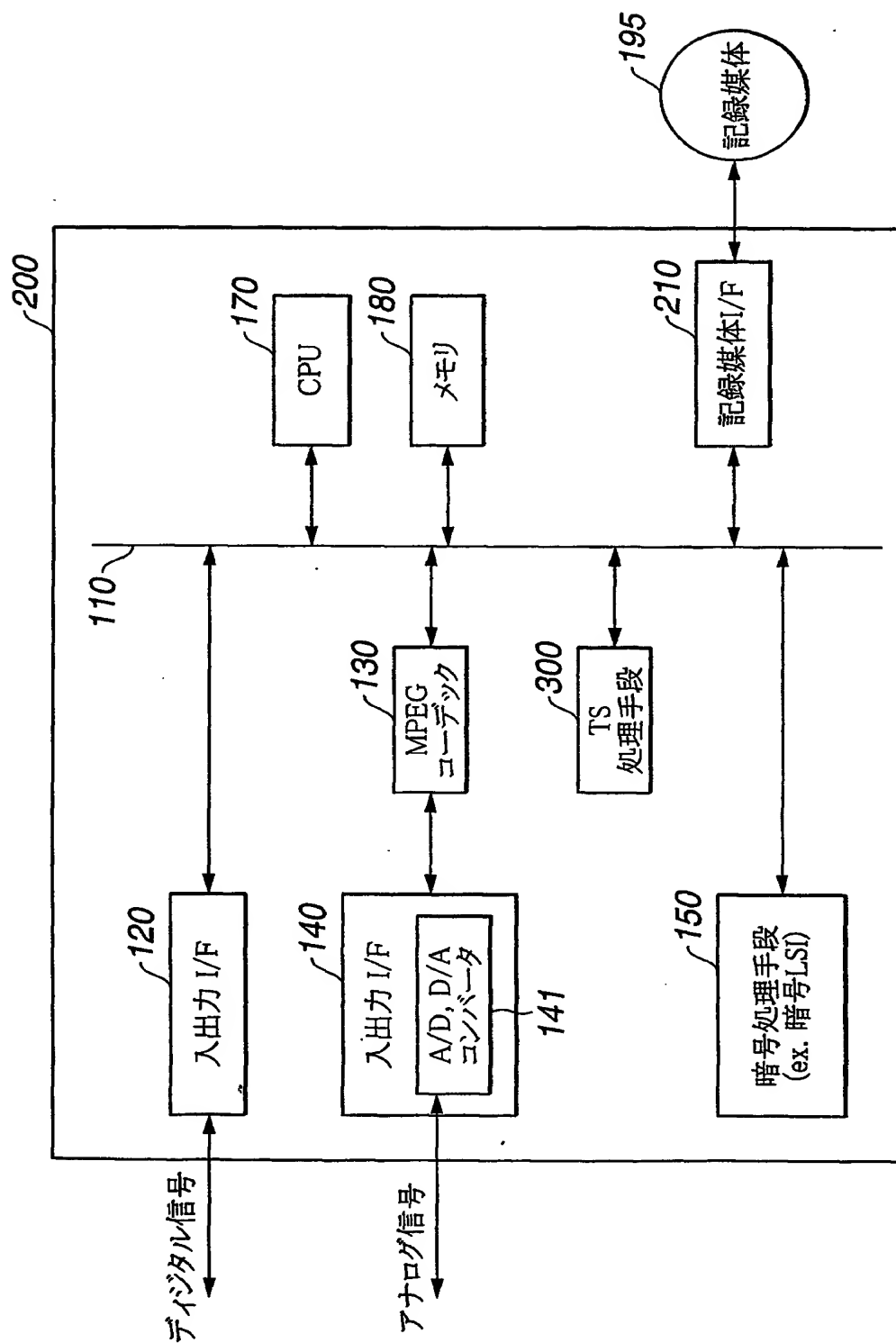


FIG.2

THIS PAGE BLANK (USPTO)

3/34

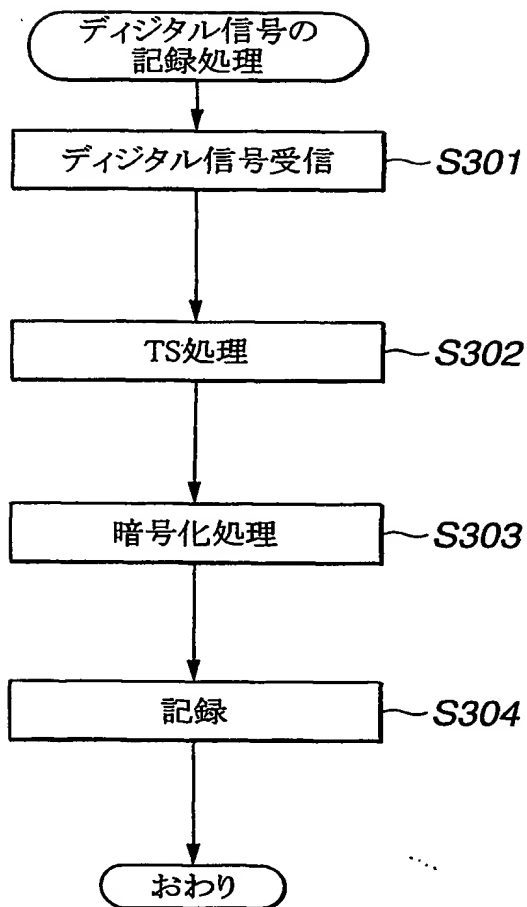


FIG.3A

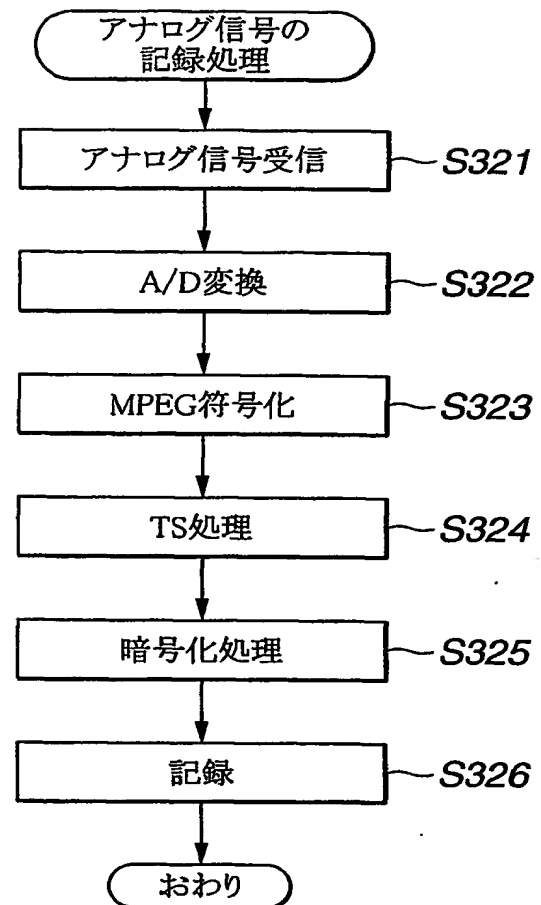


FIG.3B

THIS PAGE BLANK (USPTO)

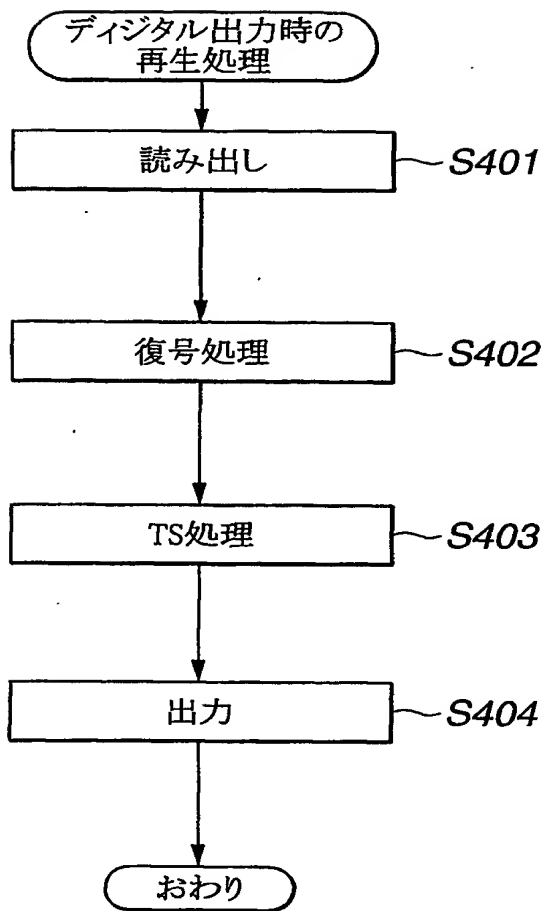


FIG.4A

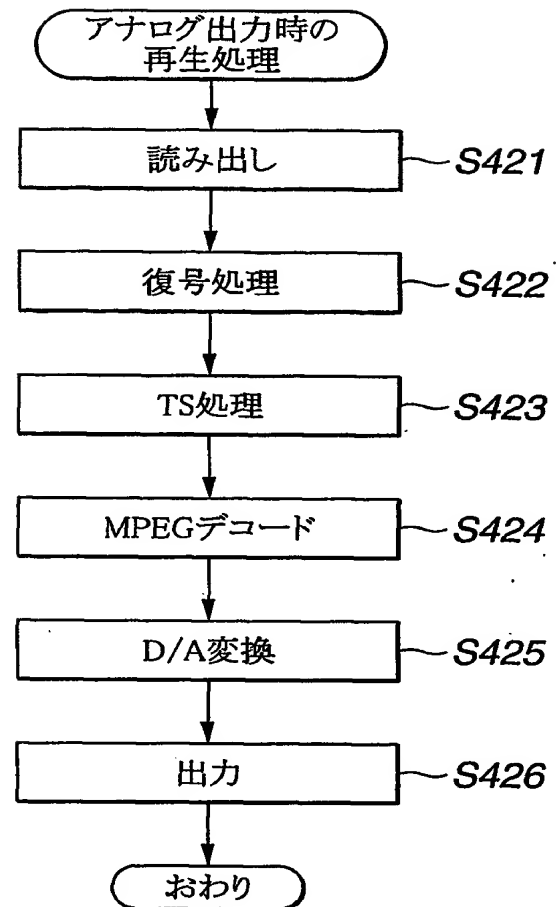


FIG.4B

THIS PAGE BLANK (USPTO)

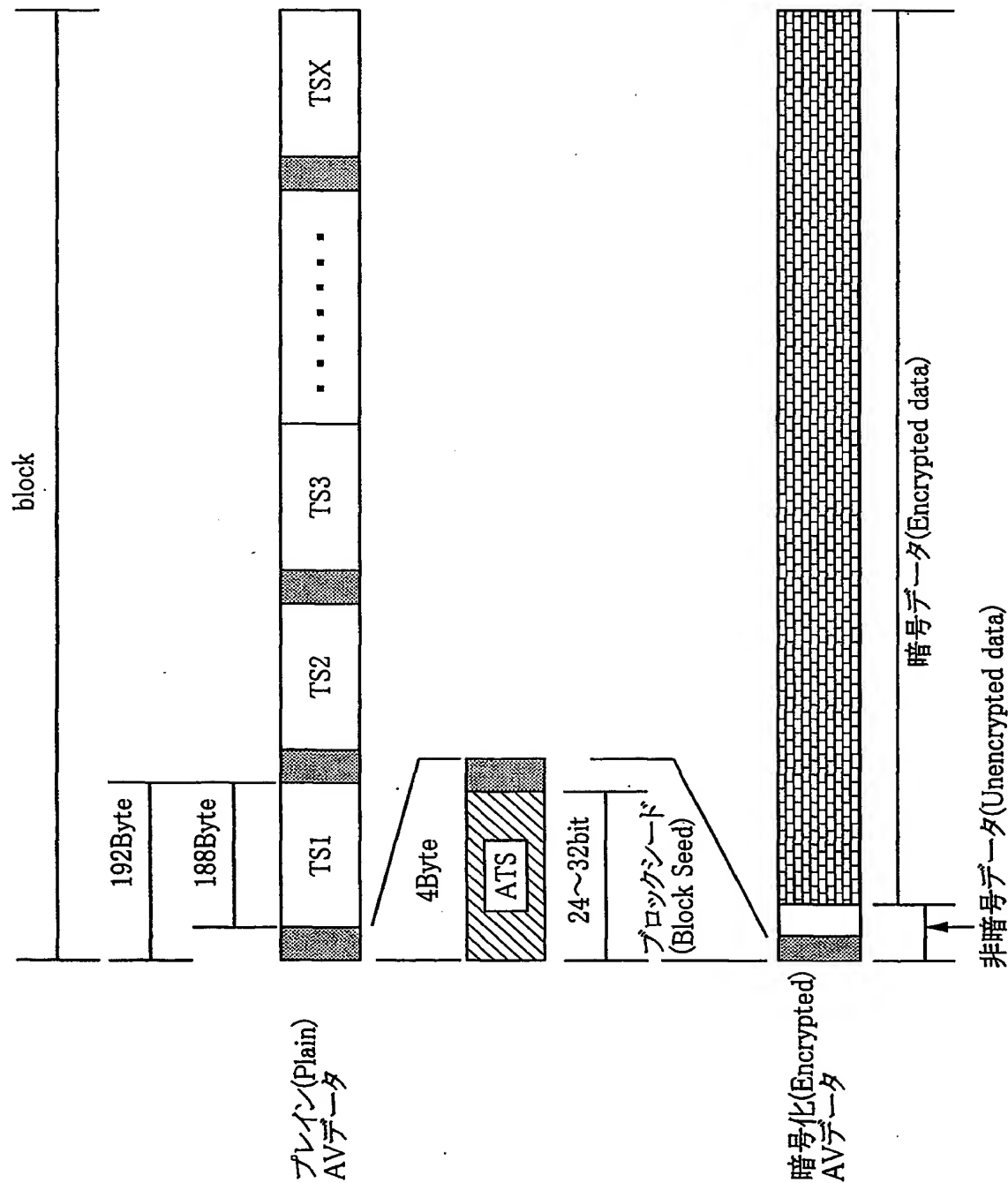


FIG.5

THIS PAGE BLANK (USPTO)

6/34

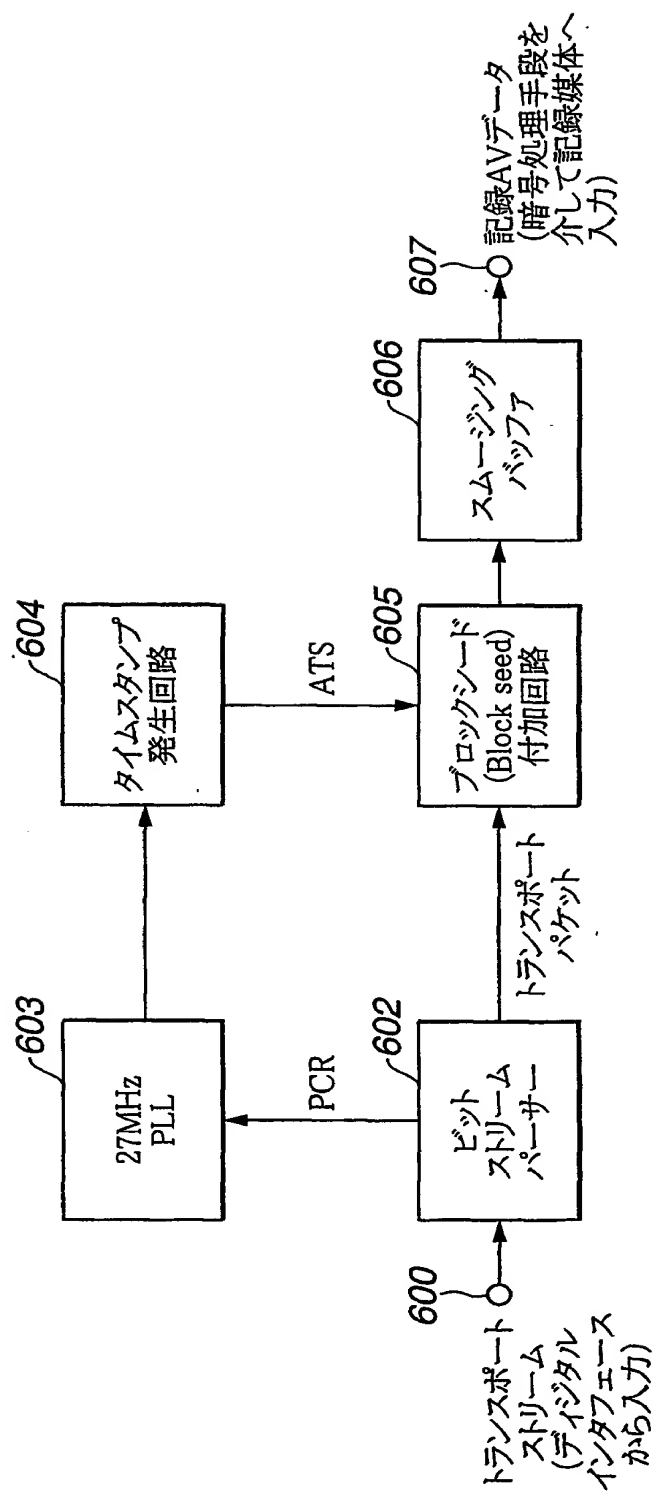


FIG.6

THIS PAGE BLANK (USPTO)

7/34

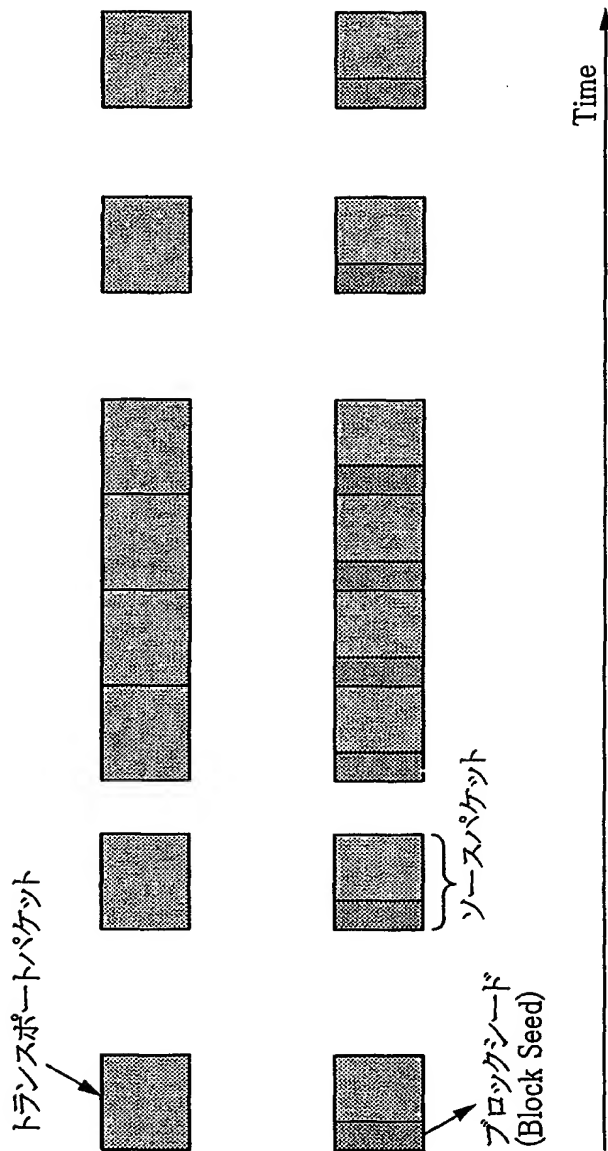


FIG.7A

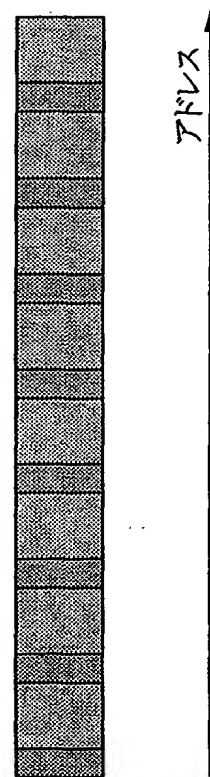
入力トランスポート
ストリーム

FIG.7B

Block seed付加器
の出力

FIG.7C

記録媒体上のAV
データ



THIS PAGE BLANK (USPTO)

8/34

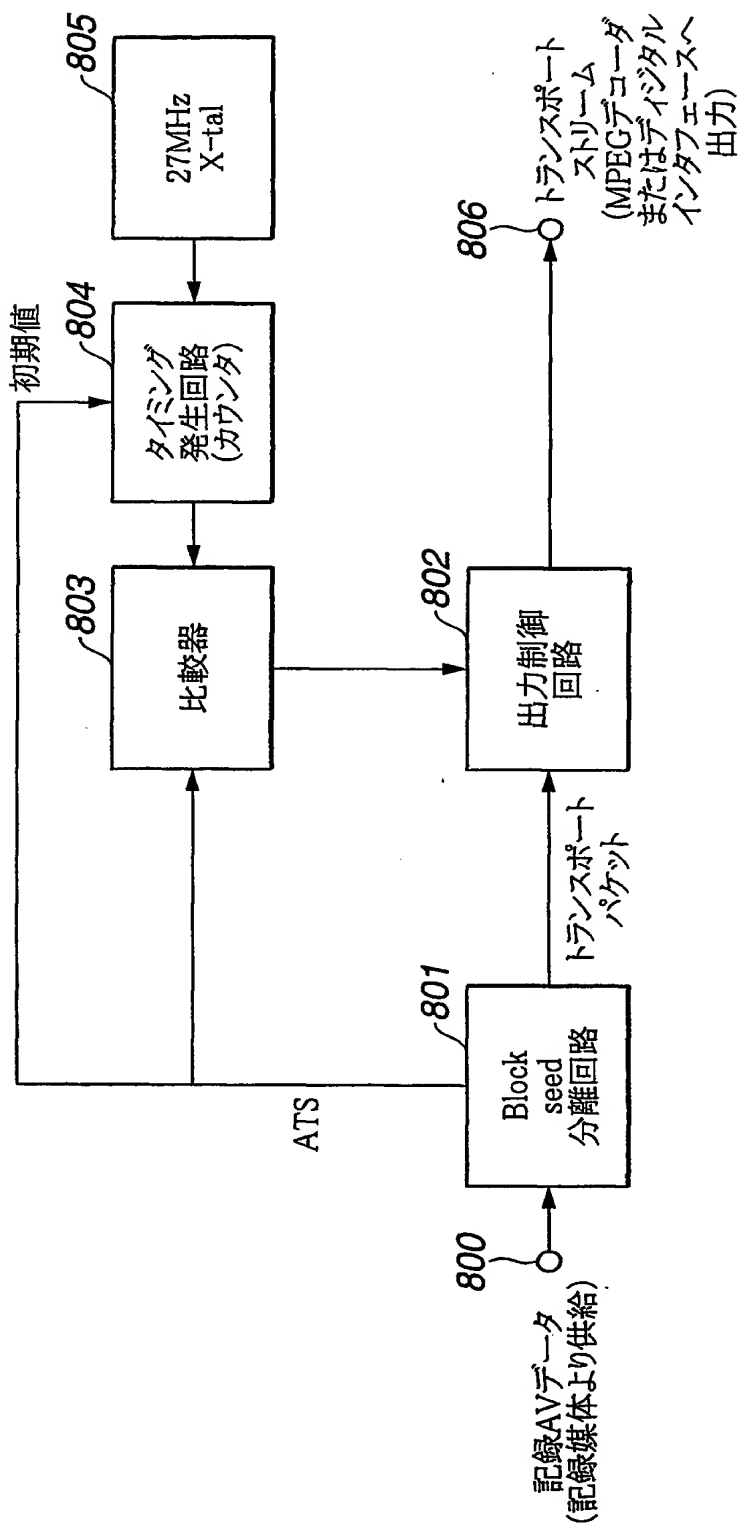


FIG.8

THIS PAGE BLANK (USPTO)

9/34

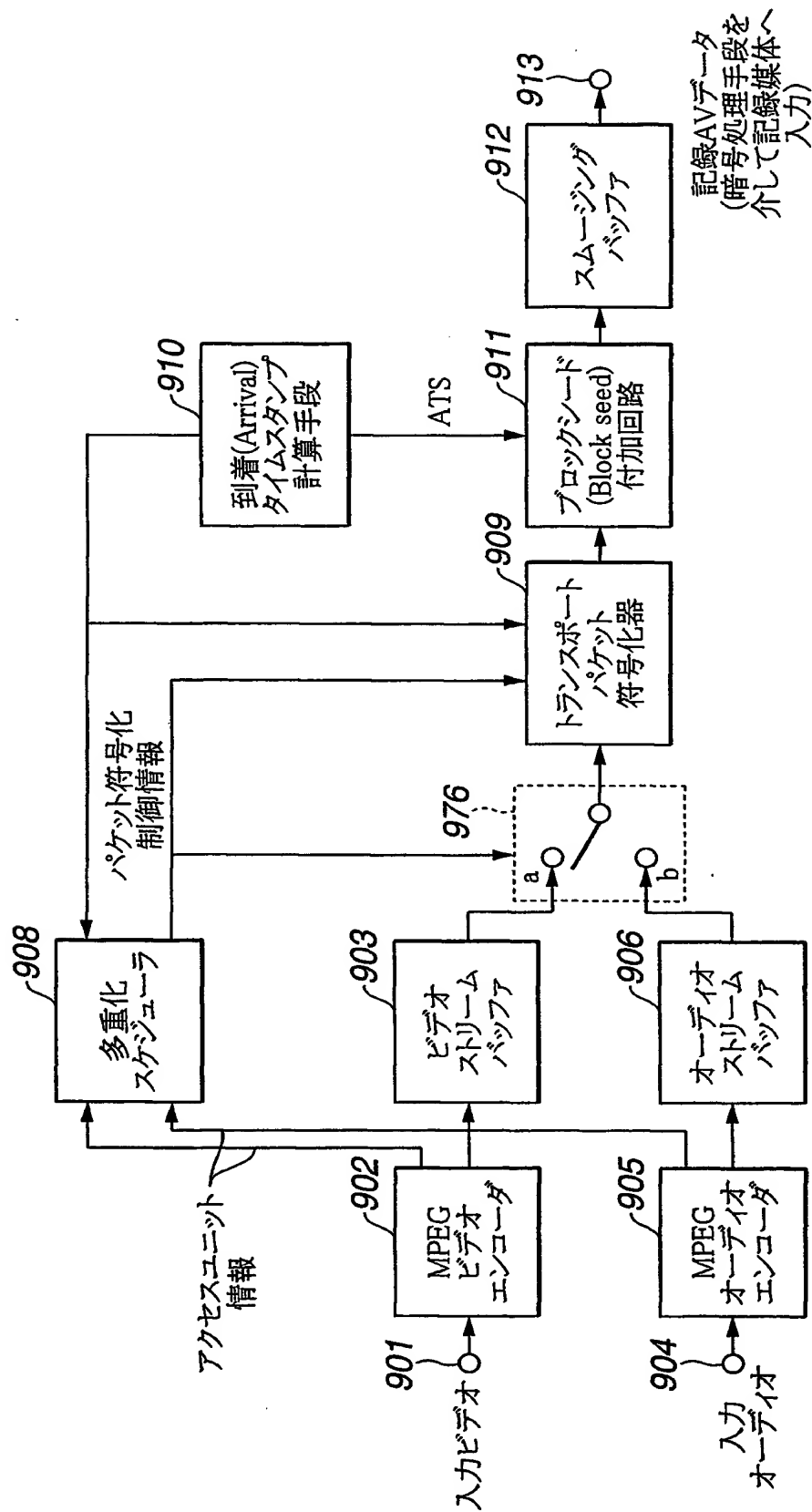


FIG.9

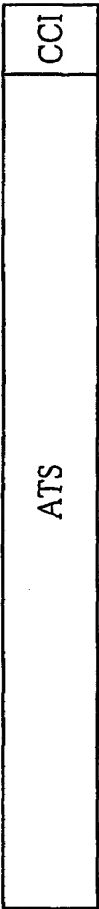
THIS PAGE BLANK (USPTO)



ブロックシード
(Block Seed)



例1
ATS 32bit



例2
ATS 30bit
CCI 2bit



例3
ATS 24bit
CCI 2bit
other info 6bit

FIG.10

THIS PAGE BLANK (USPTO)

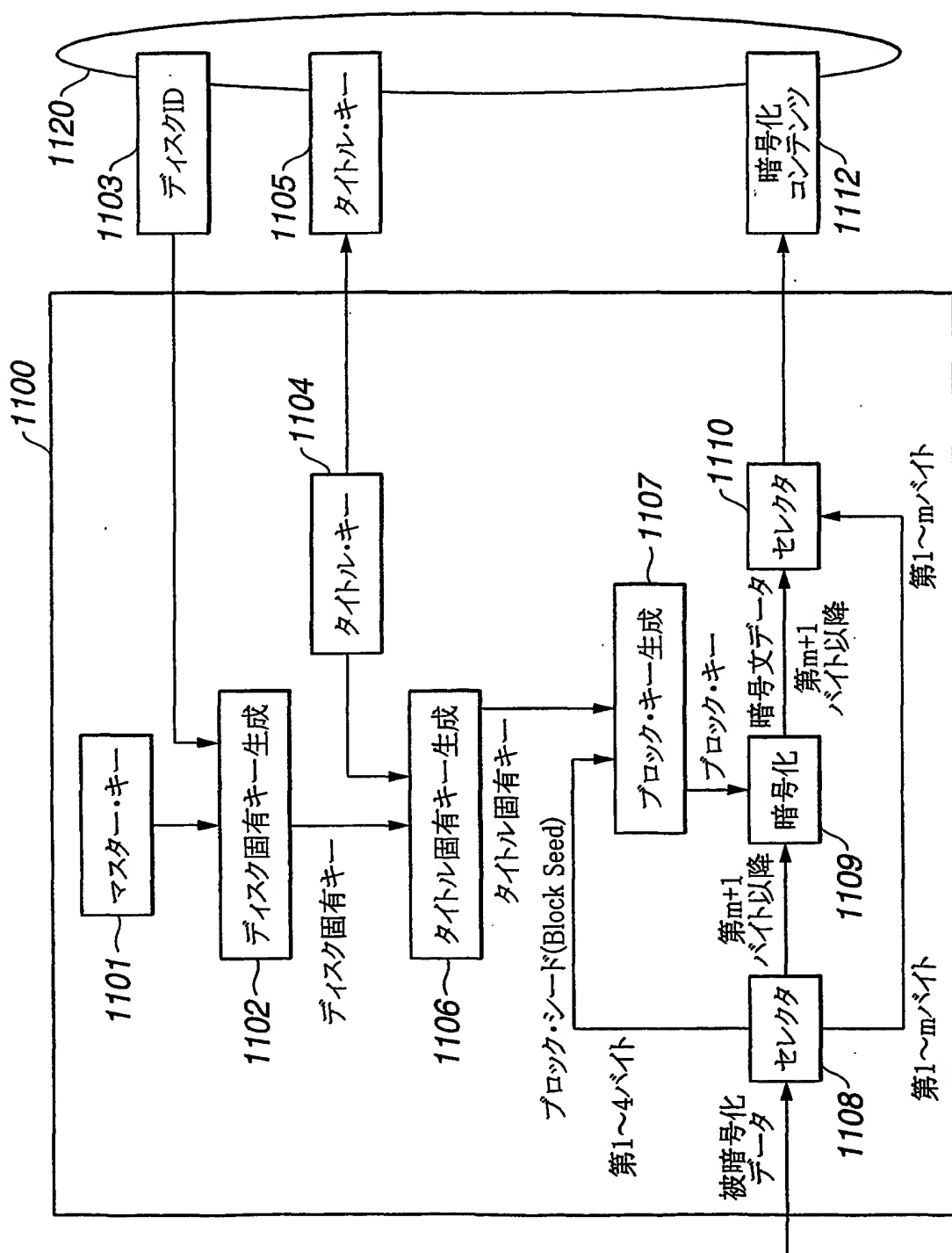


FIG.11

THIS PAGE BLANK (USPTO)

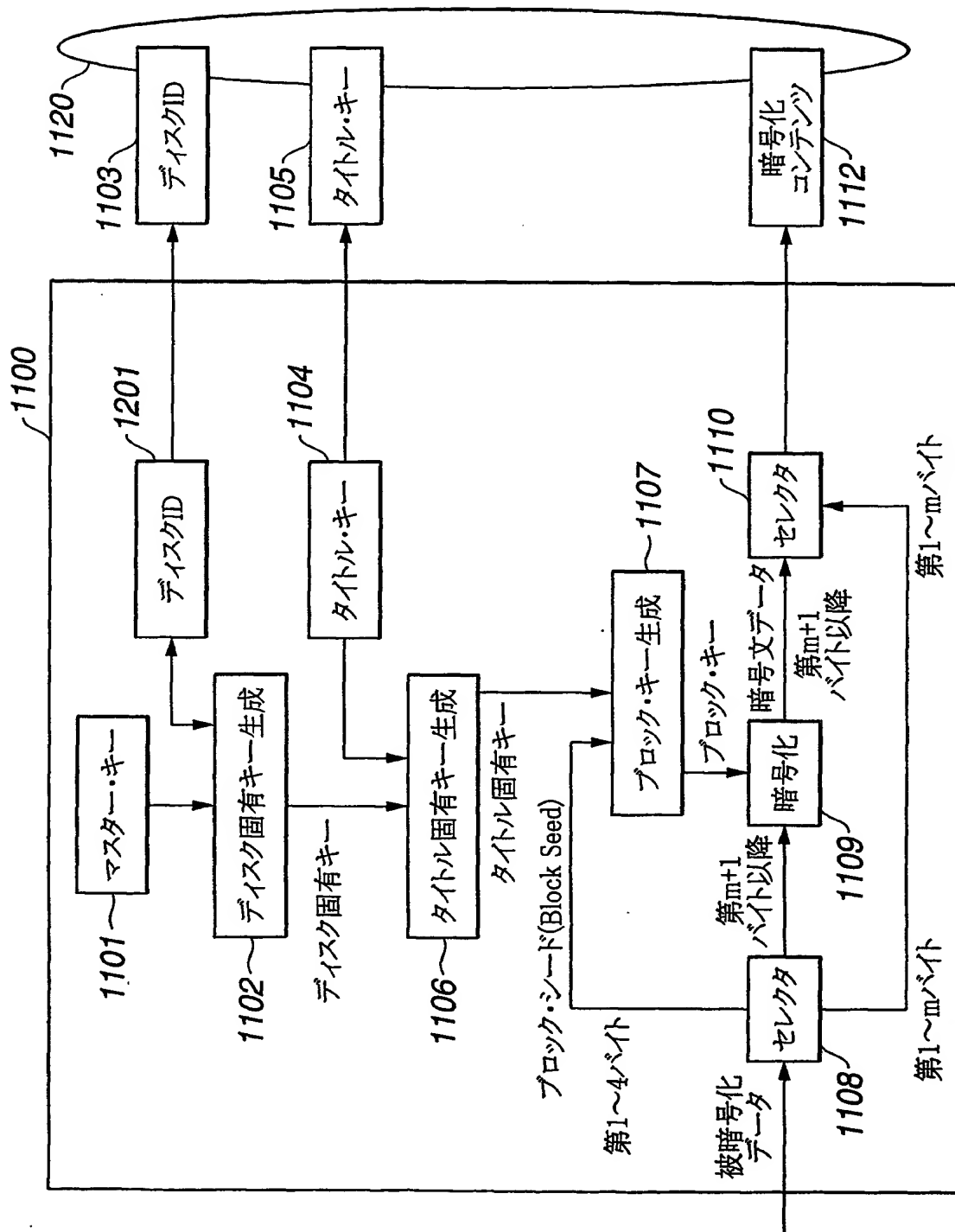


FIG.12

THIS PAGE BLANK (USPTO)

13/34

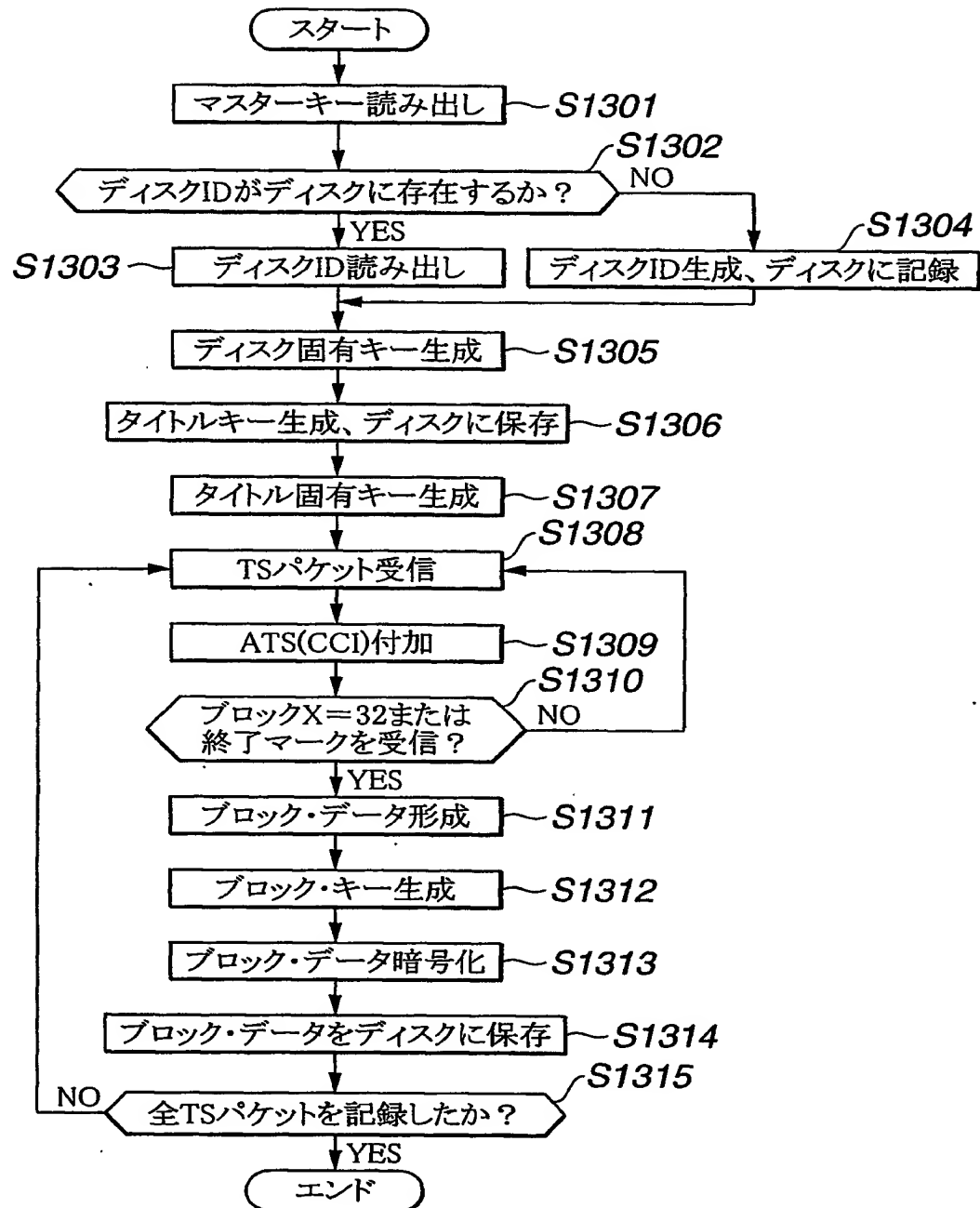


FIG.13

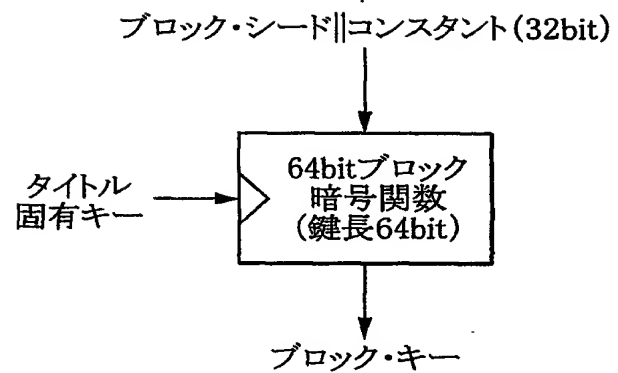
THIS PAGE BLANK (USPTO)

14/34

例1

ブロック・キー生成例

入力
ブロック・シード (32bit)
タイトル固有キー (64bit)



出力
ブロック・キー (64bit)

例2

タイトル固有キー||ブロック・シード

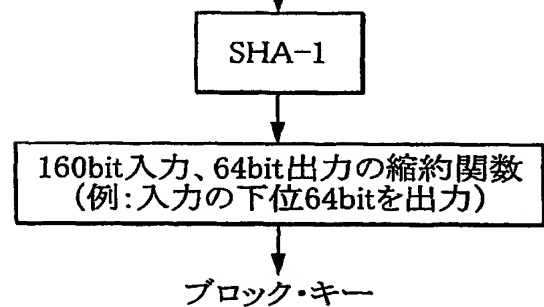


FIG.14

THIS PAGE BLANK (USPTO)

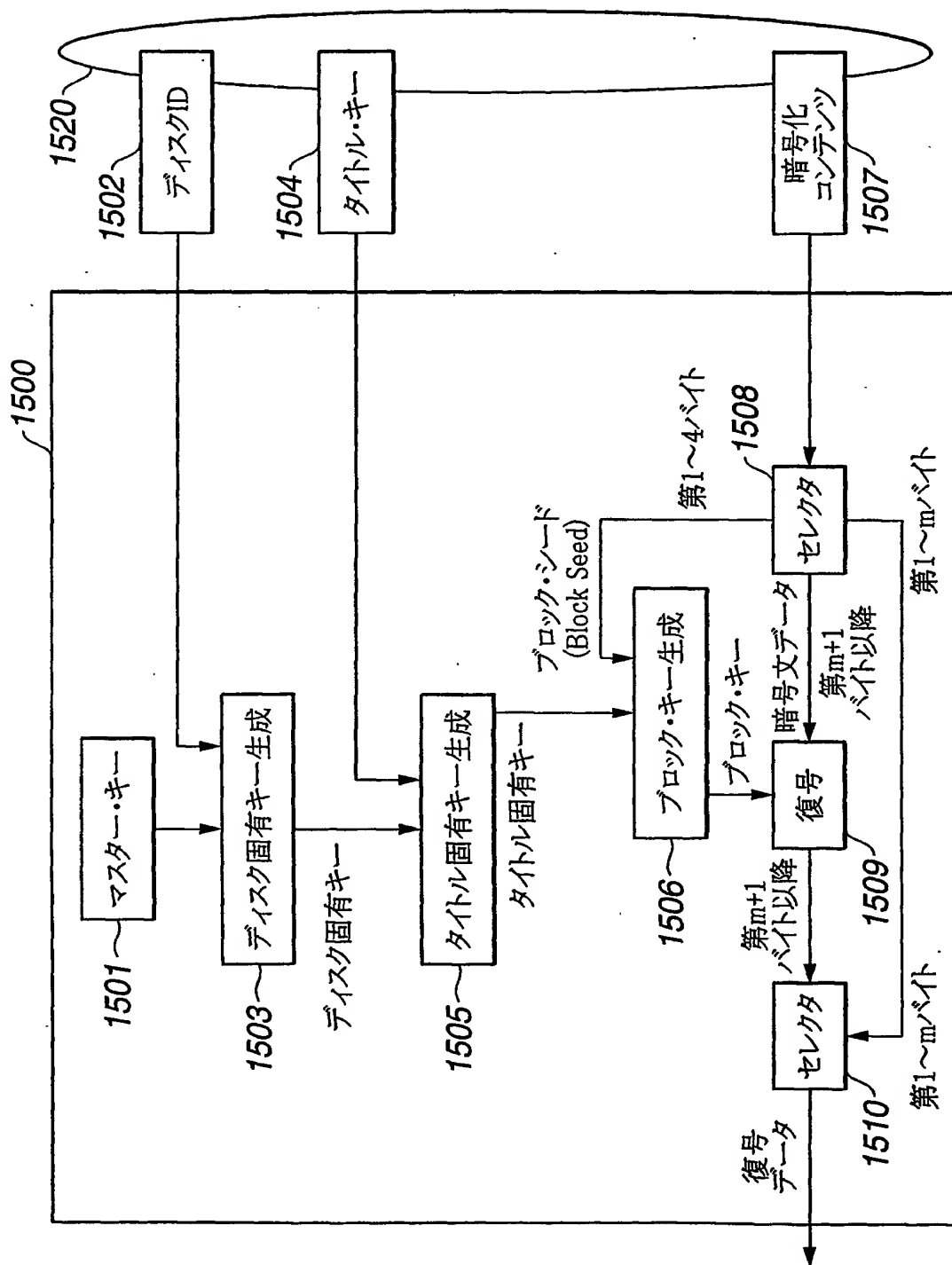


FIG.15

THIS PAGE BLANK (USPTO)

16/34

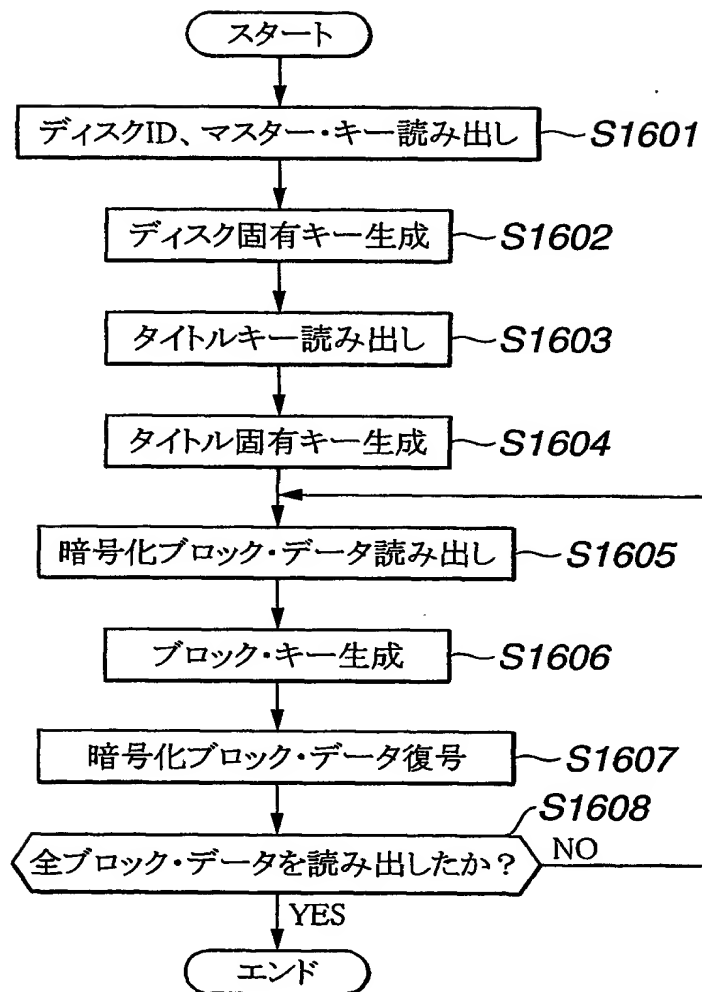


FIG.16

THIS PAGE BLANK (USPTO)

17/34

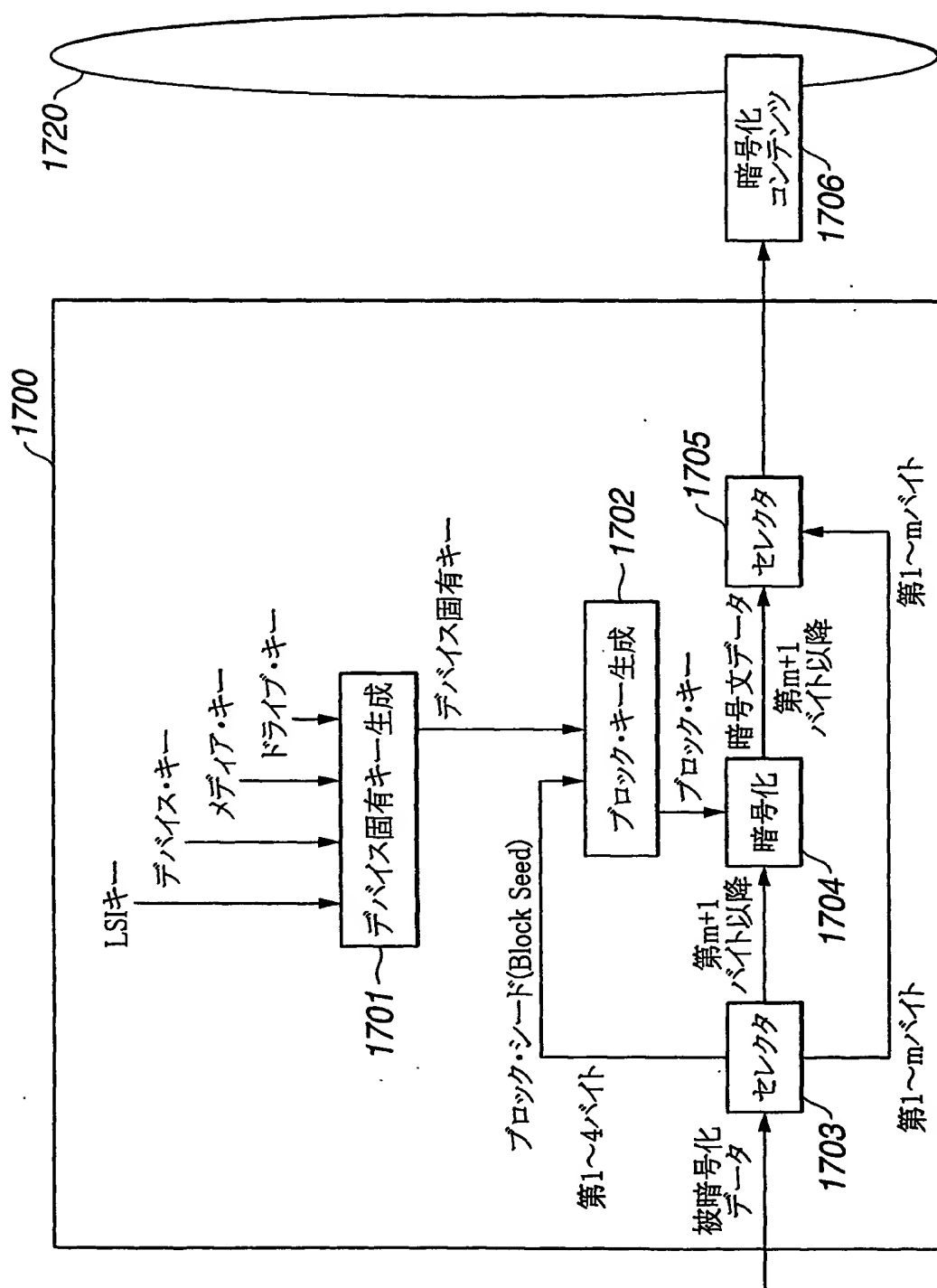


FIG.17

THIS PAGE BLANK (USPTO)

18/34

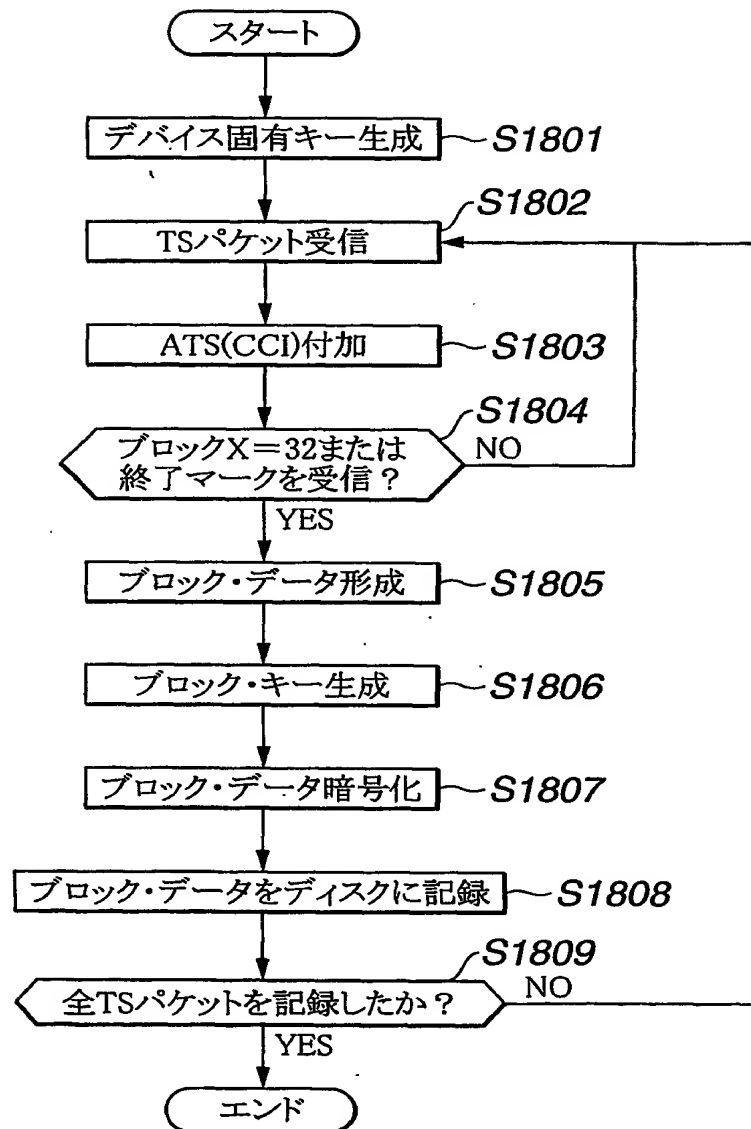


FIG.18

THIS PAGE BLANK (USPTO)

19/34

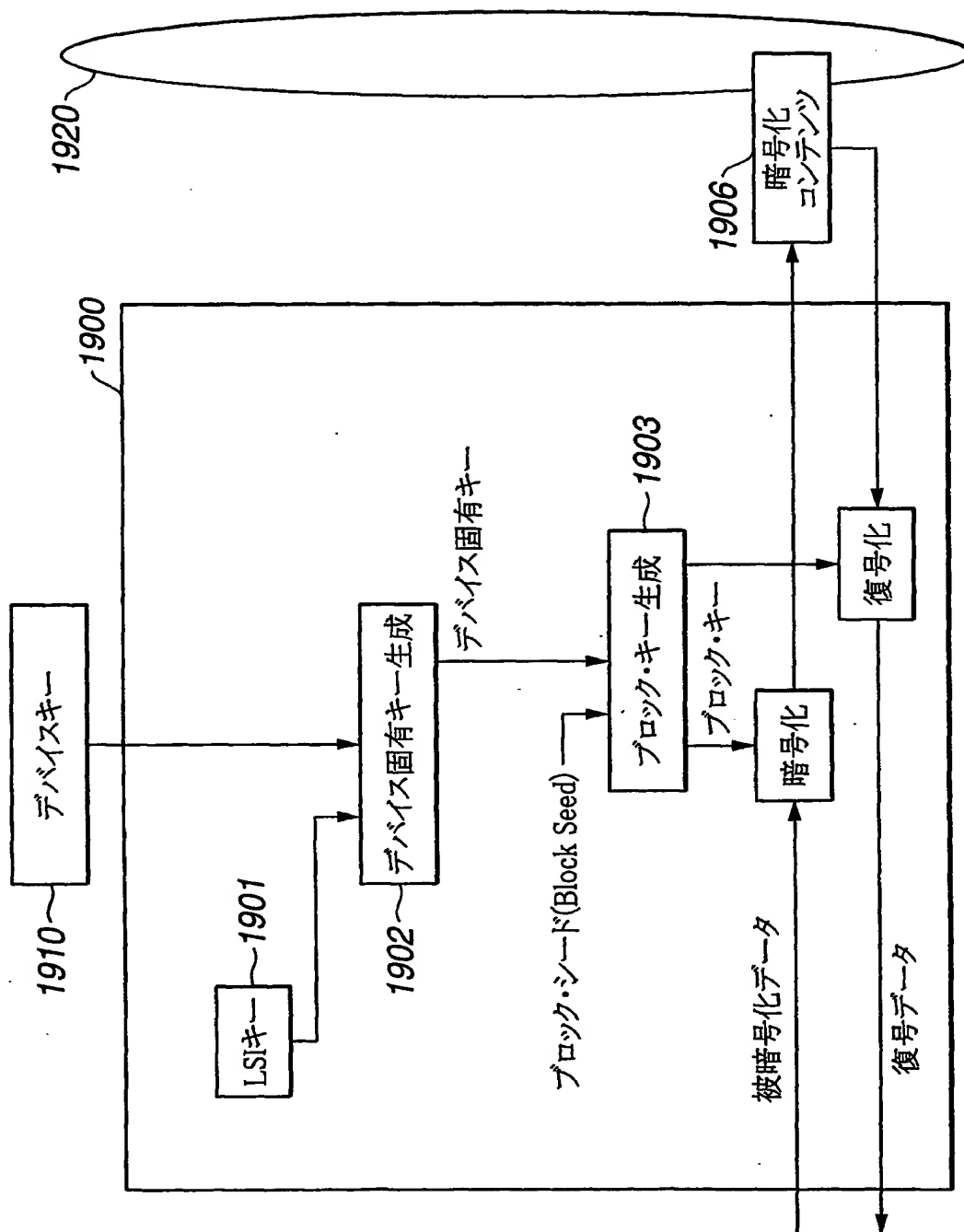


FIG.19

THIS PAGE BLANK (USPTO)

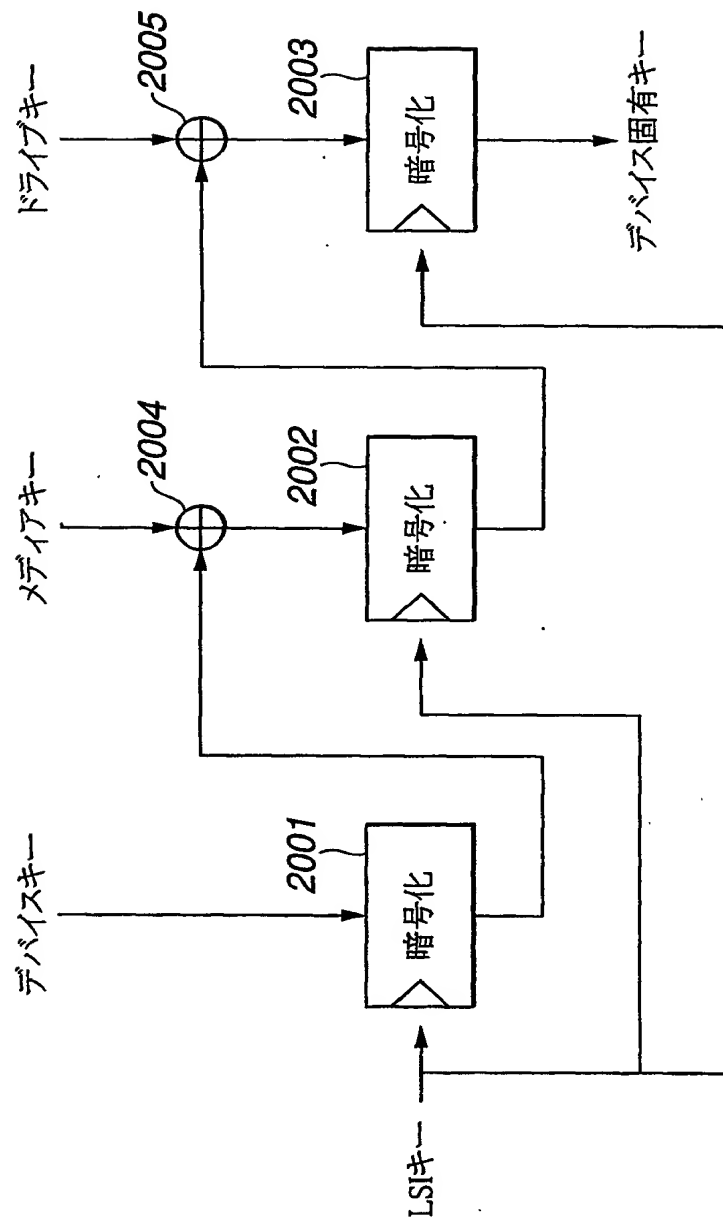


FIG.20

THIS PAGE BLANK (USPTO)

21/34

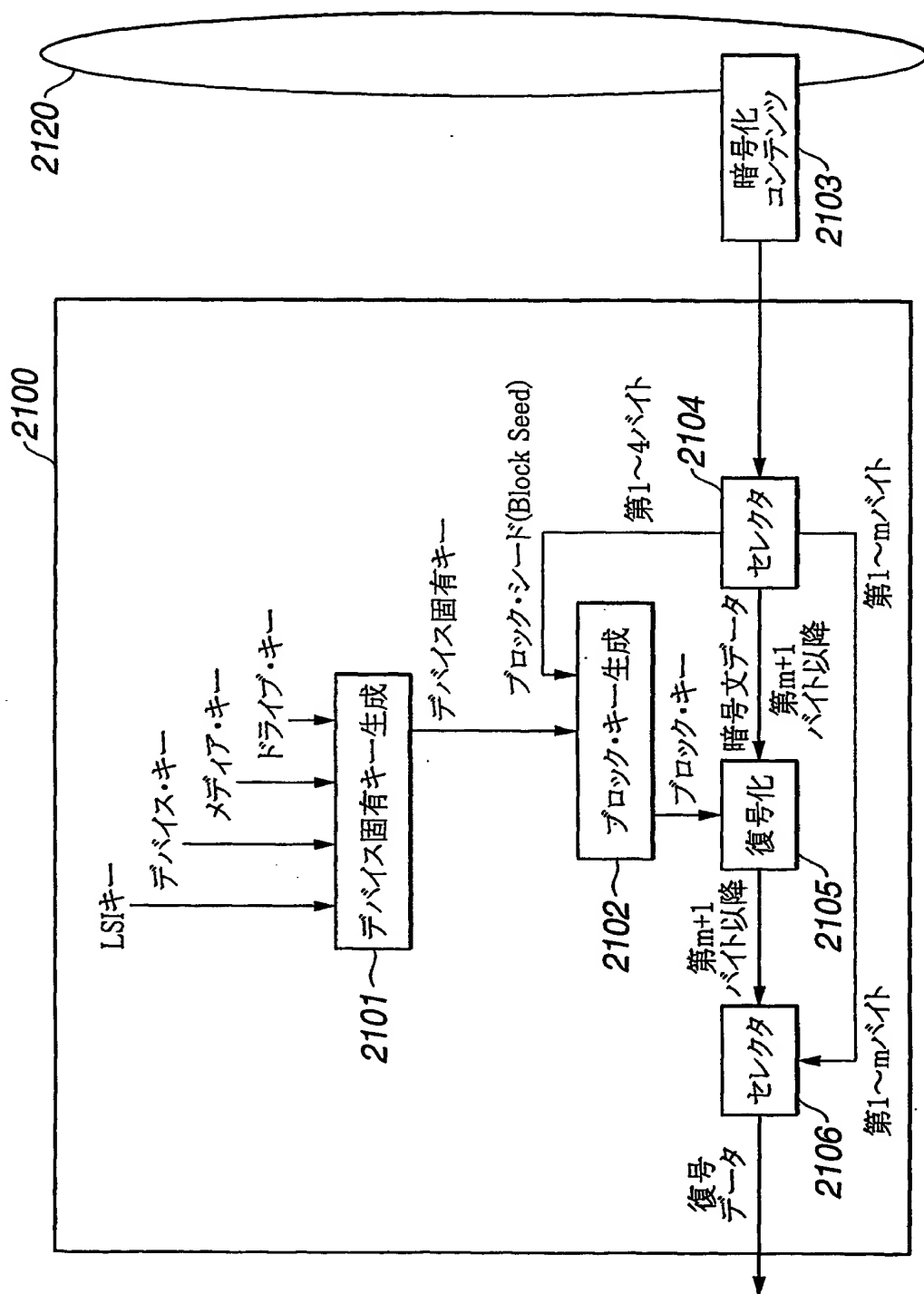


FIG.21

THIS PAGE BLANK (USPTO)

22/34

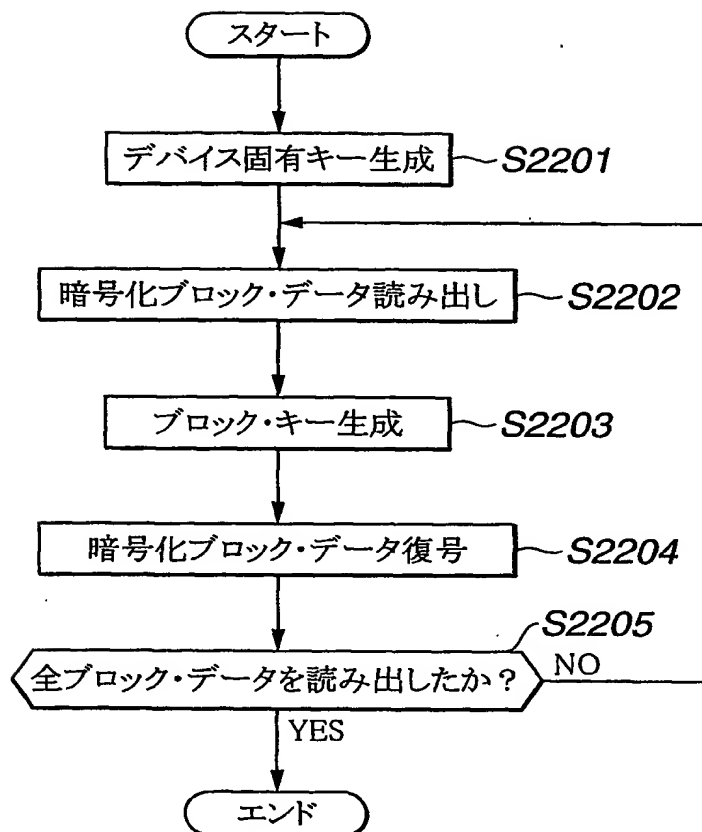


FIG.22

THIS PAGE BLANK (USPTO)

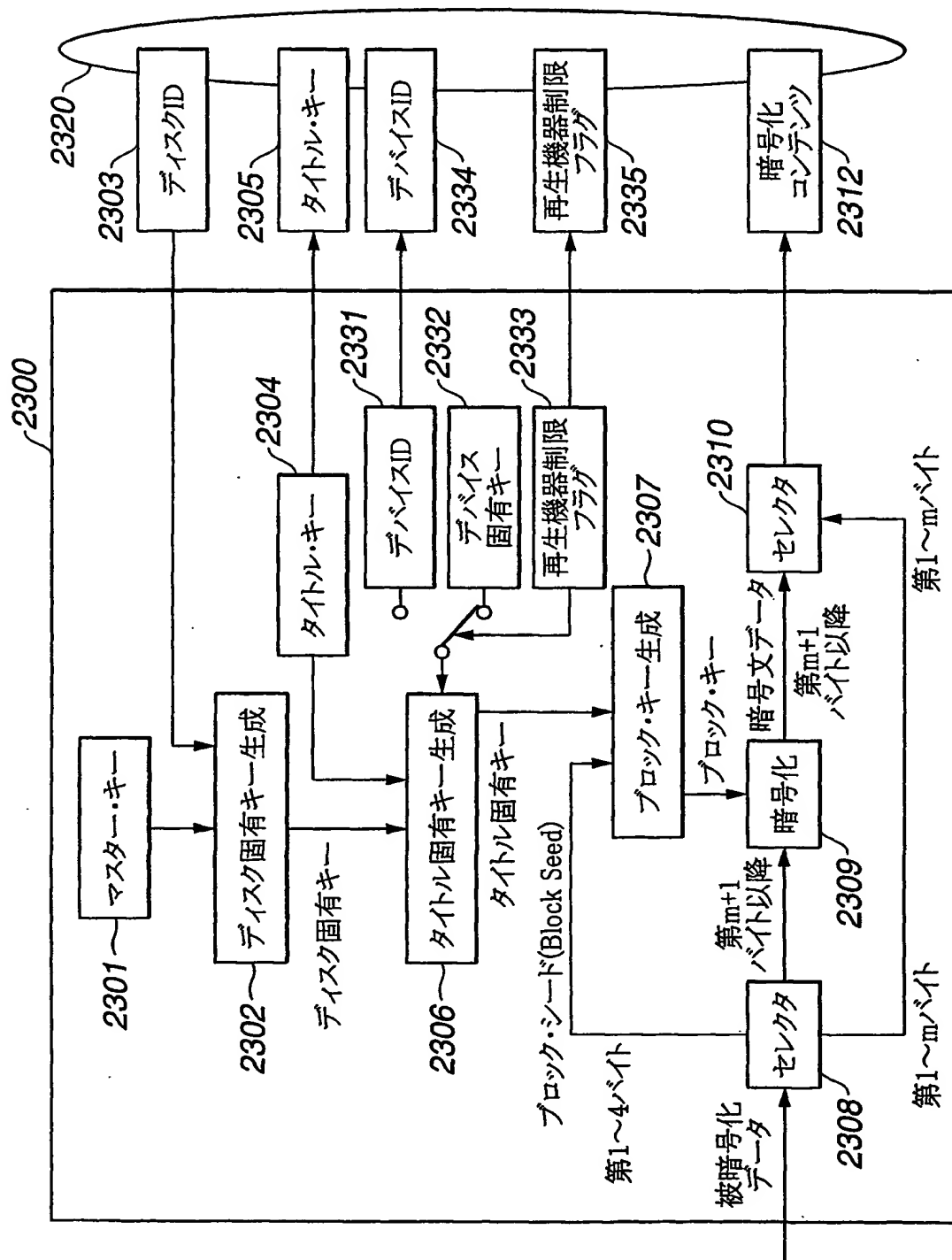


FIG. 23

THIS PAGE BLANK (USPTO)

24/34

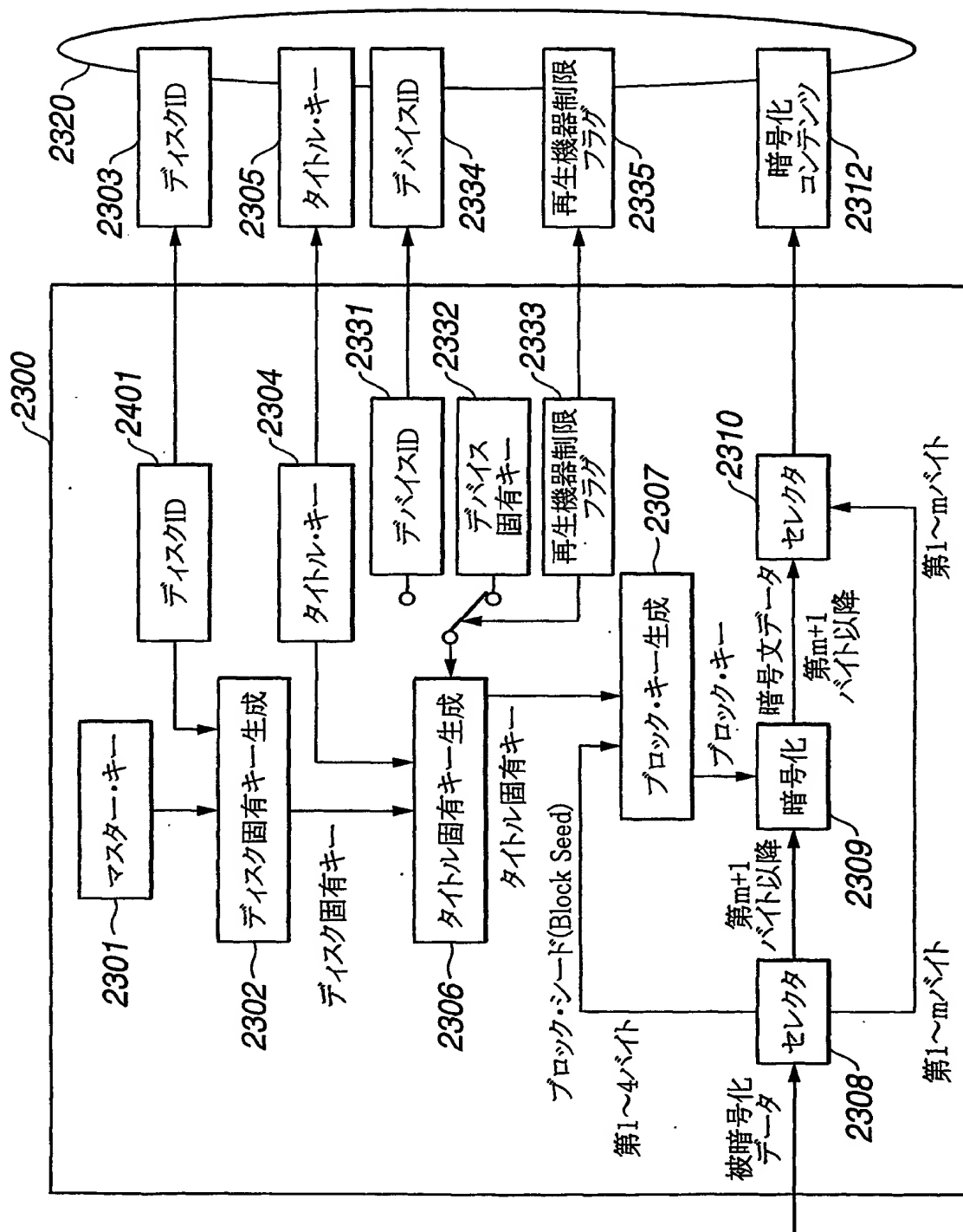


FIG. 24

THIS PAGE BLANK (USPTO)

25/34

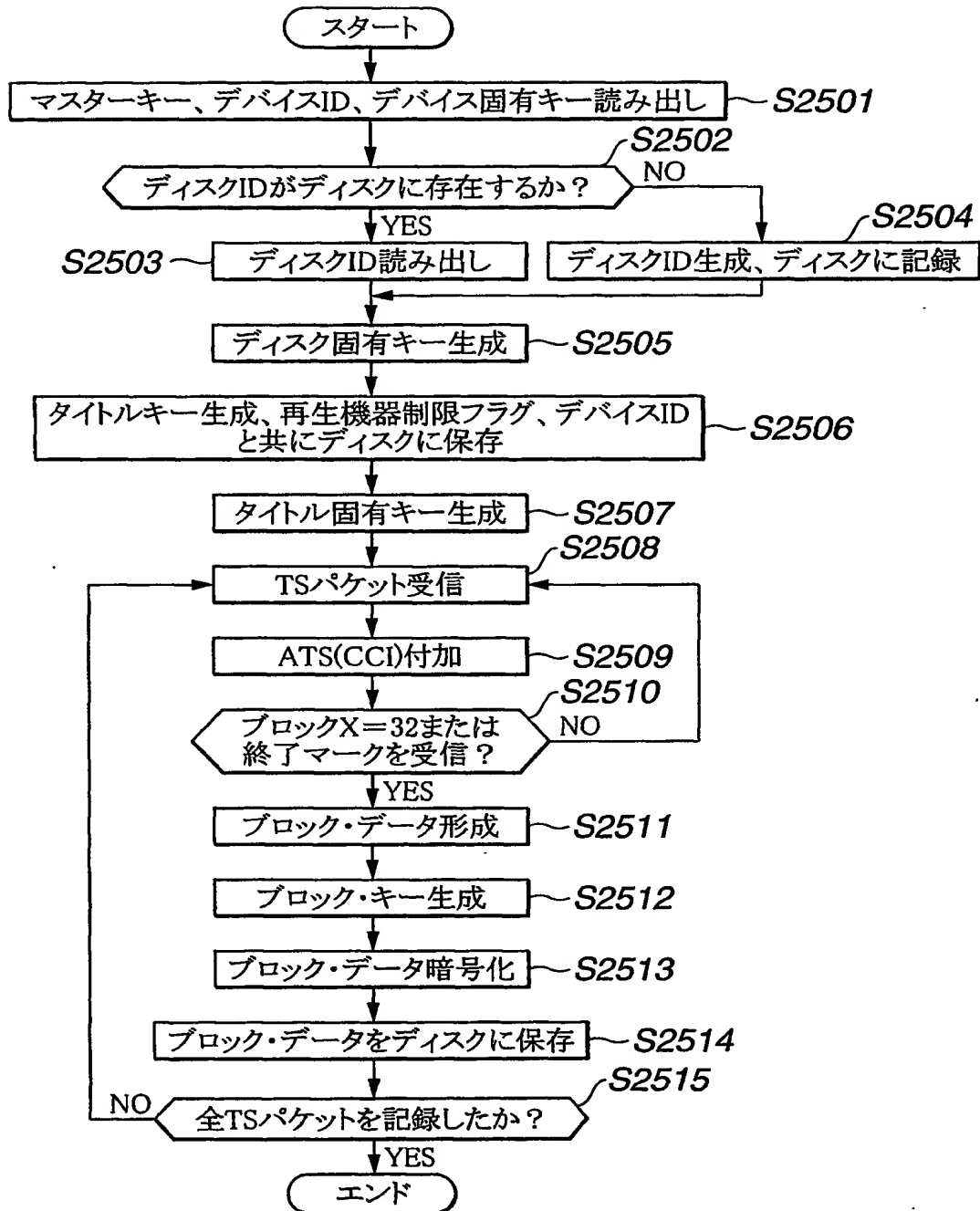


FIG.25

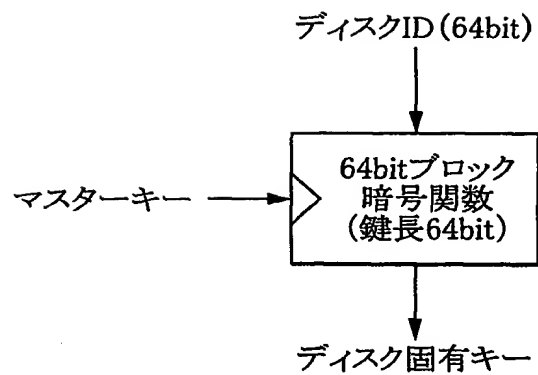
THIS PAGE BLANK (USPTO)

26/34

例1

ディスク固有キー生成例

入力
マスターキー (64bit)
ディスクID (64bit)



出力
ディスク固有キー (64bit)

例2

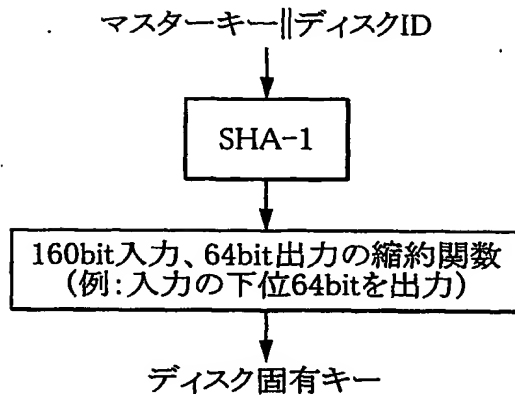


FIG.26

THIS PAGE BLANK (USPTO)

27/34

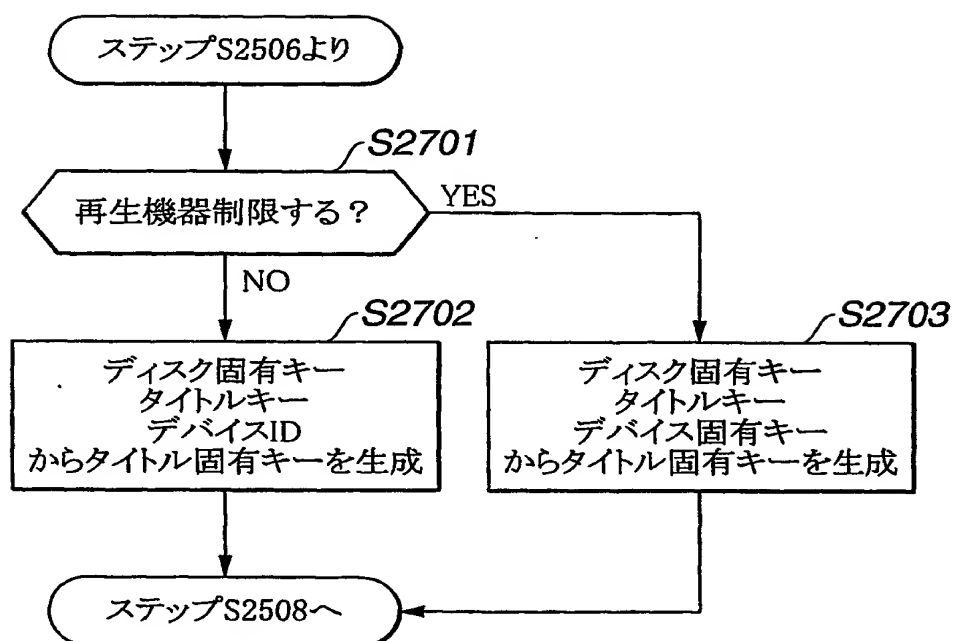


FIG.27

THIS PAGE BLANK (USPTO)

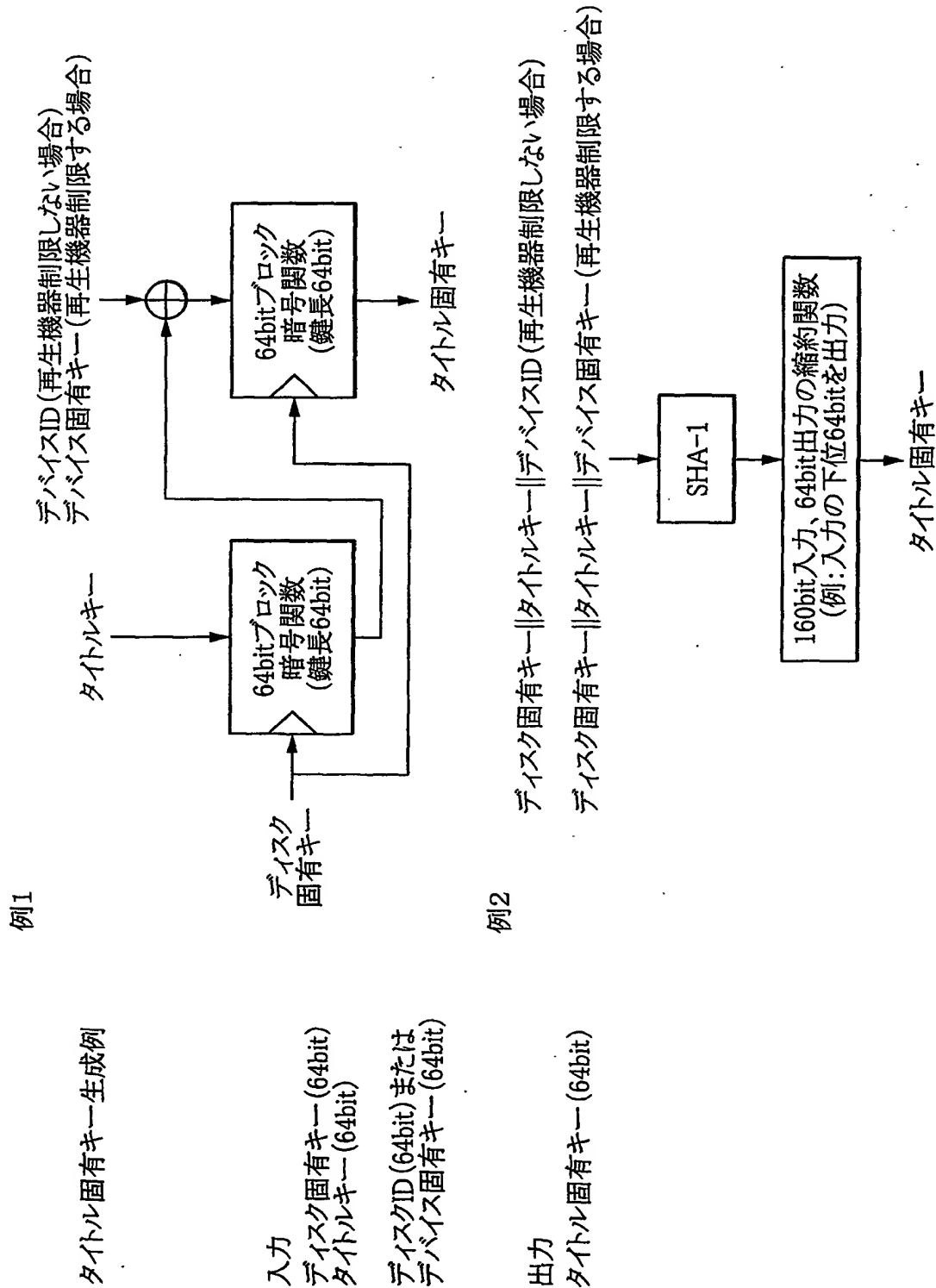


FIG.28

THIS PAGE BLANK (USPTO)

29/34

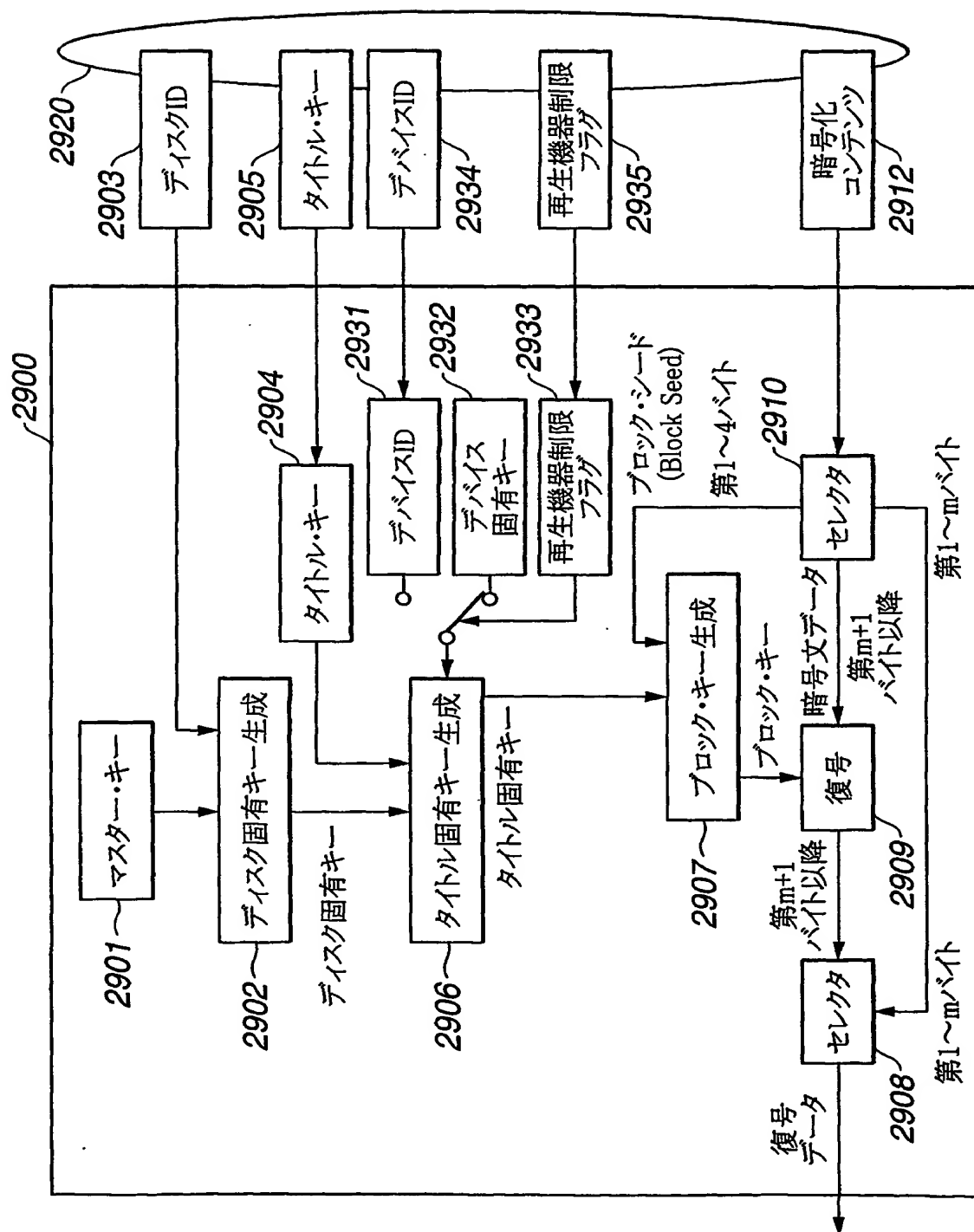


FIG. 29

THIS PAGE BLANK (USPTO)

30/34

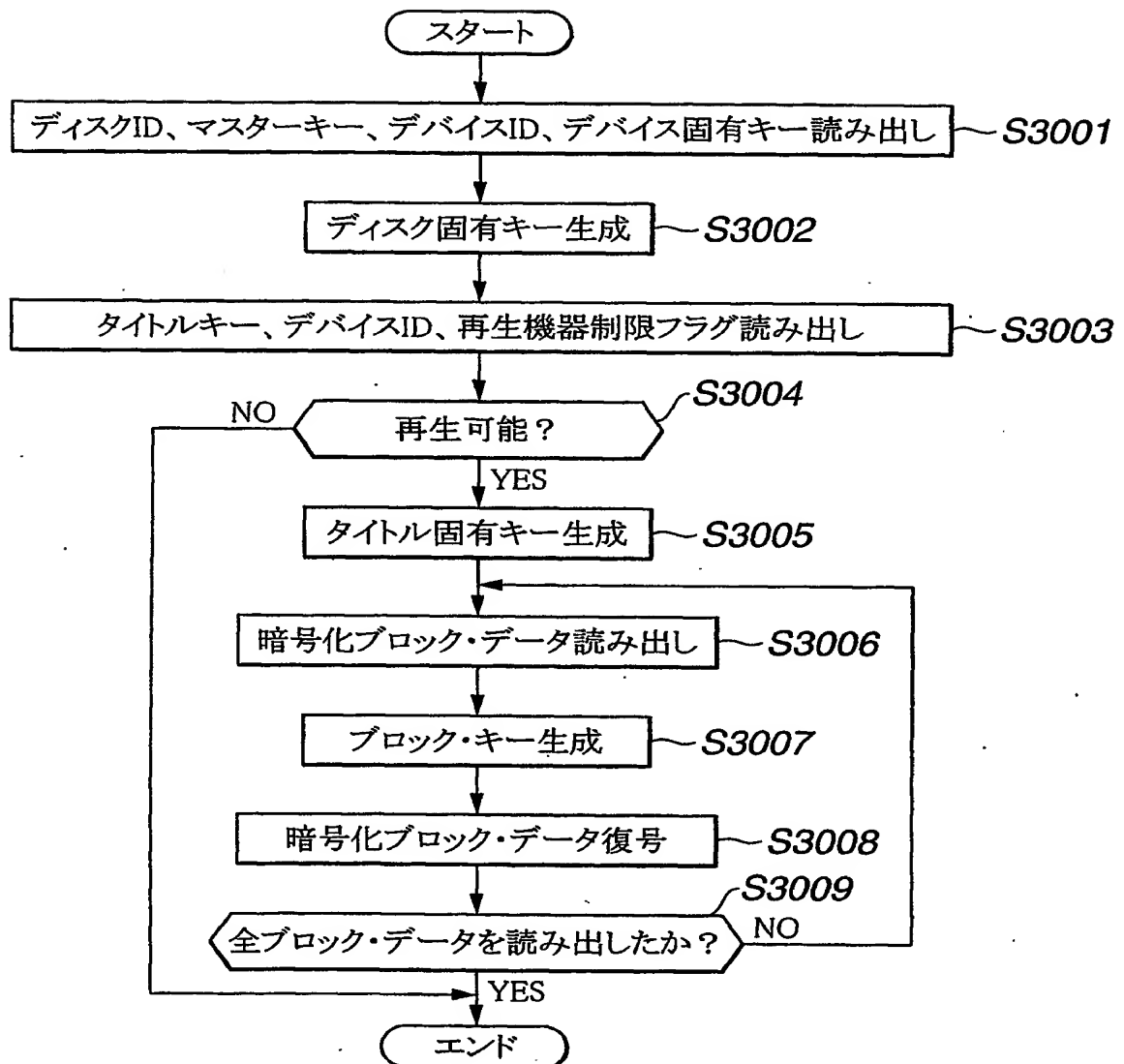


FIG.30

THIS PAGE BLANK (USPTO)

31/34

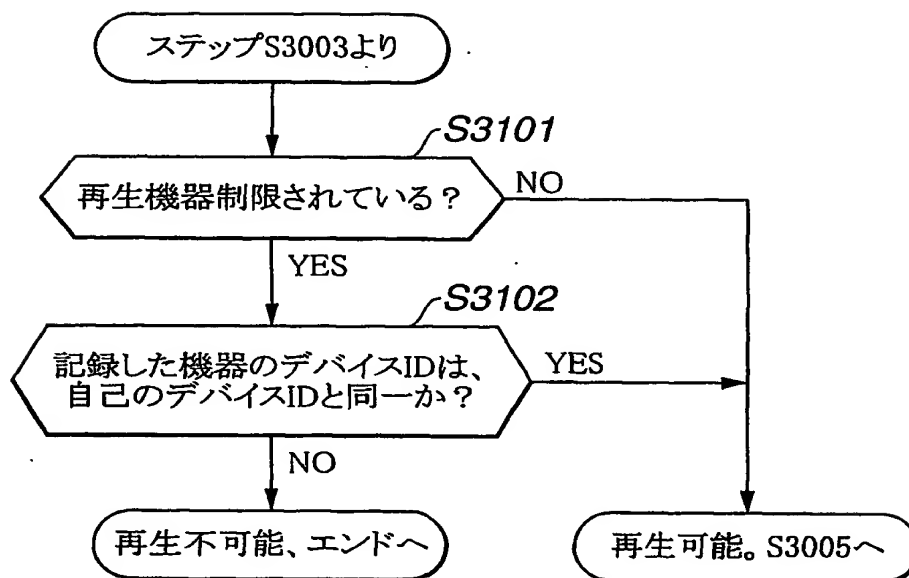


FIG.31

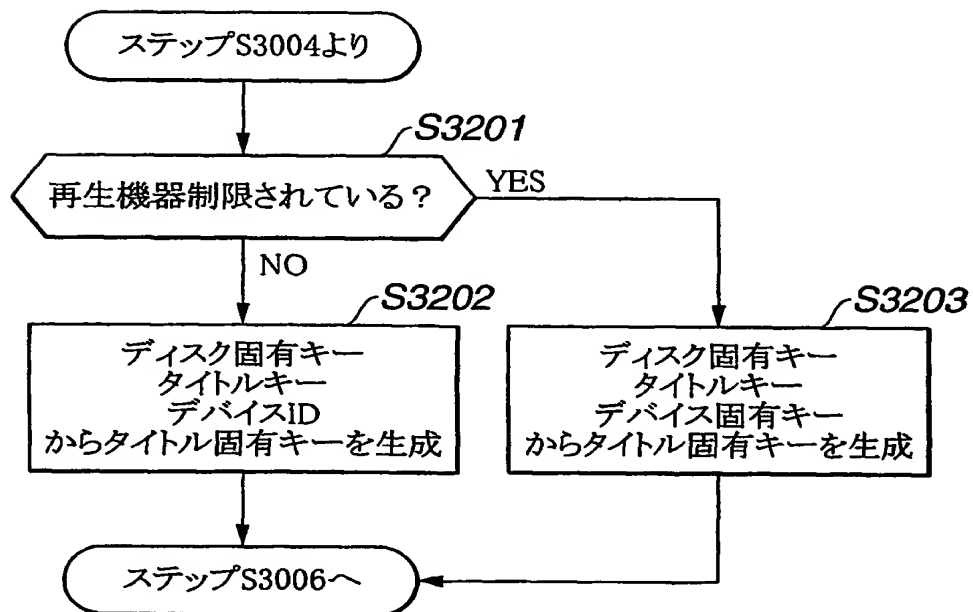


FIG.32

THIS PAGE BLANK (USPTO)

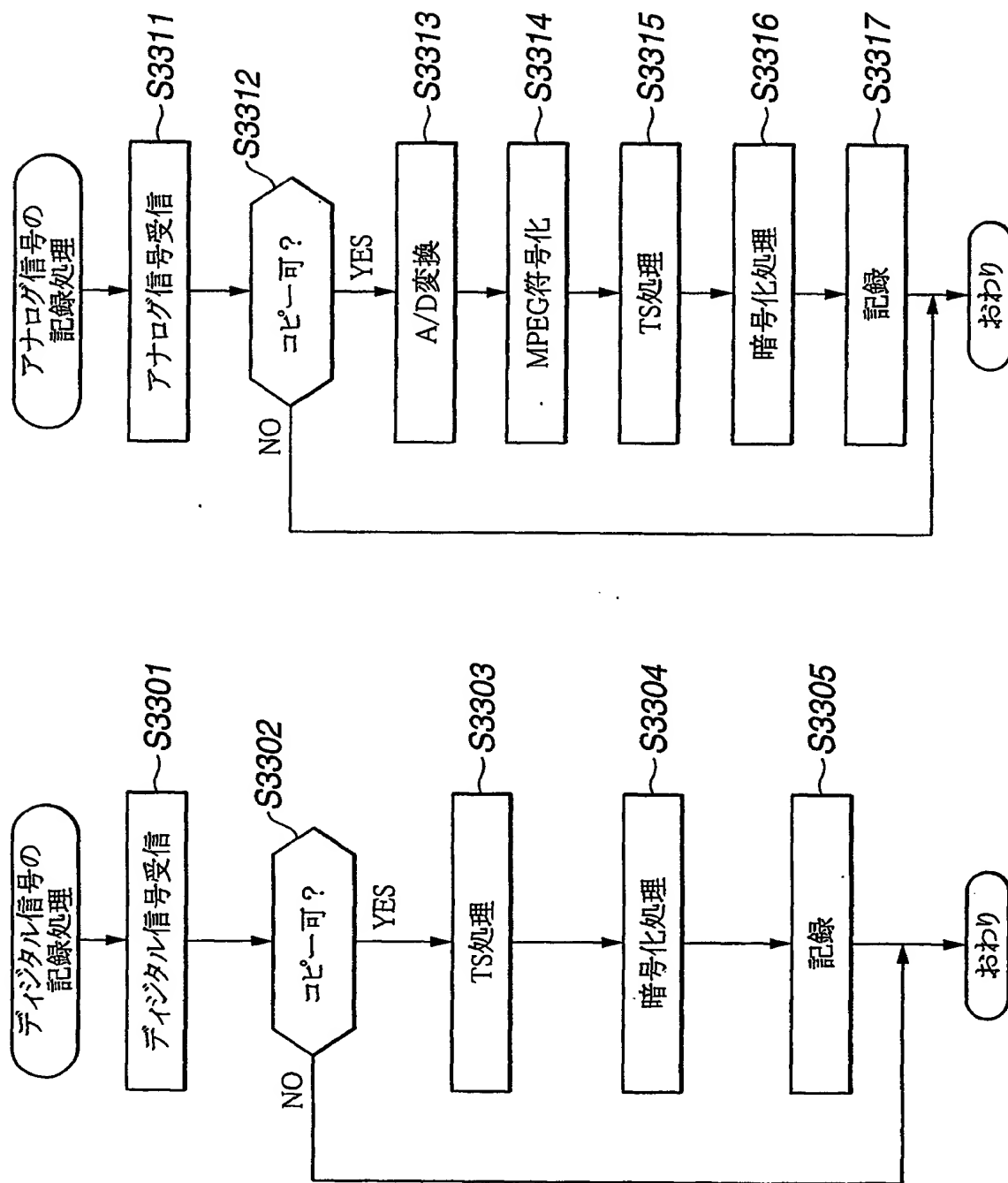


FIG. 33B

FIG. 33A

THIS PAGE BLANK (USPTO)

33/34

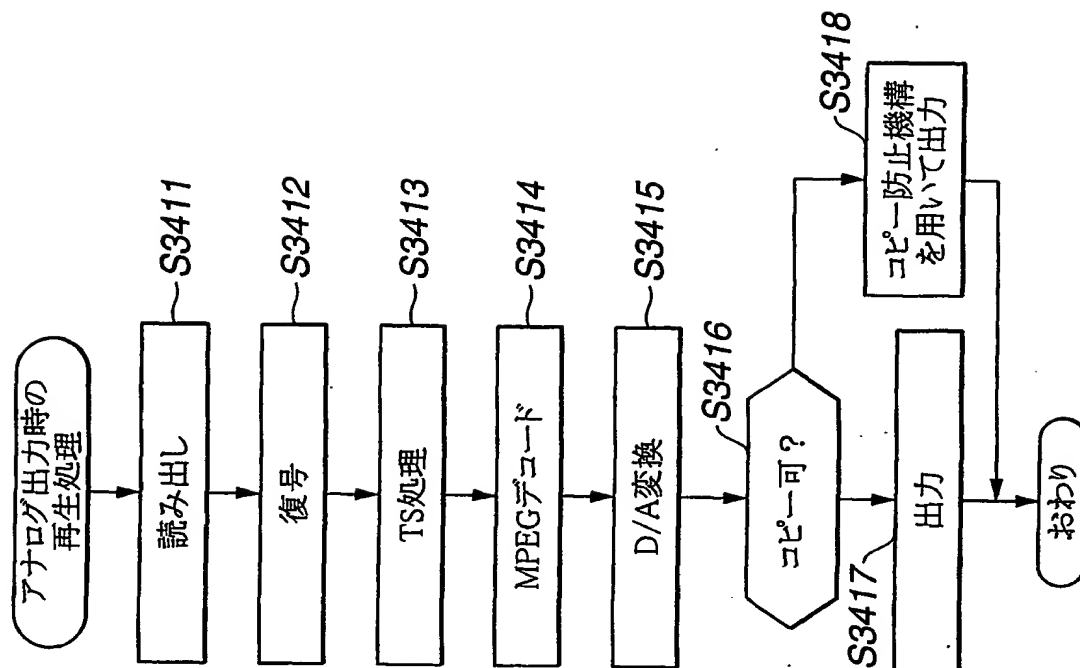
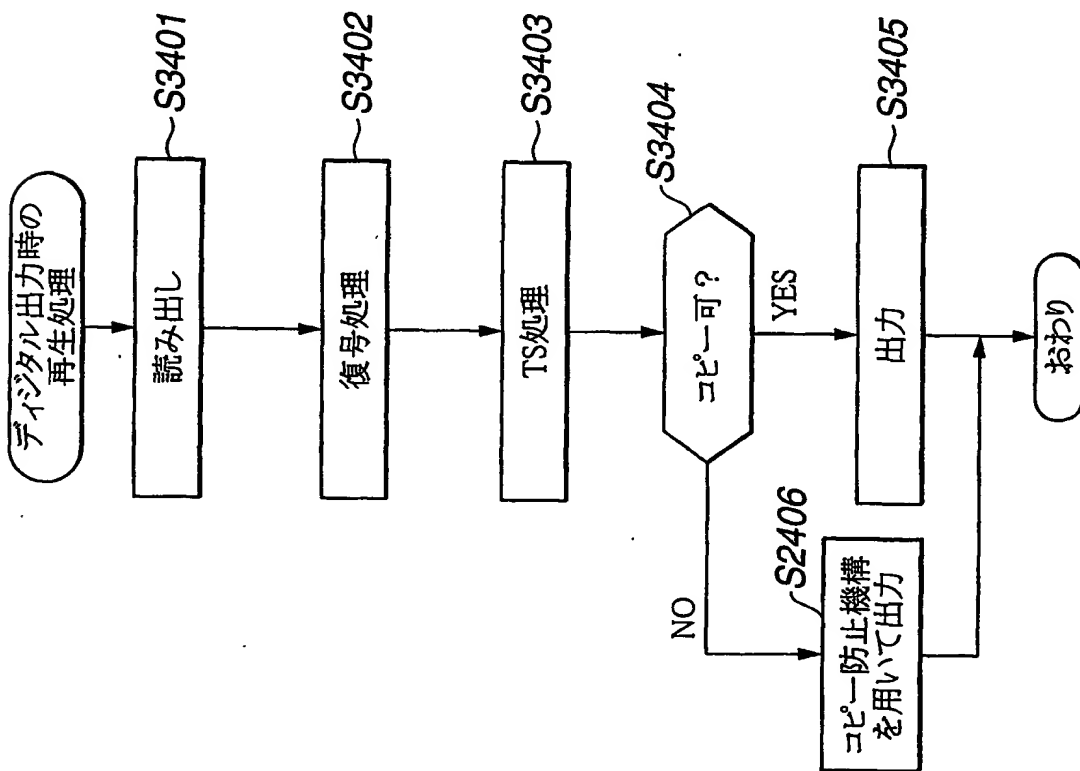


FIG. 34B



THIS PAGE BLANK (USPTO)

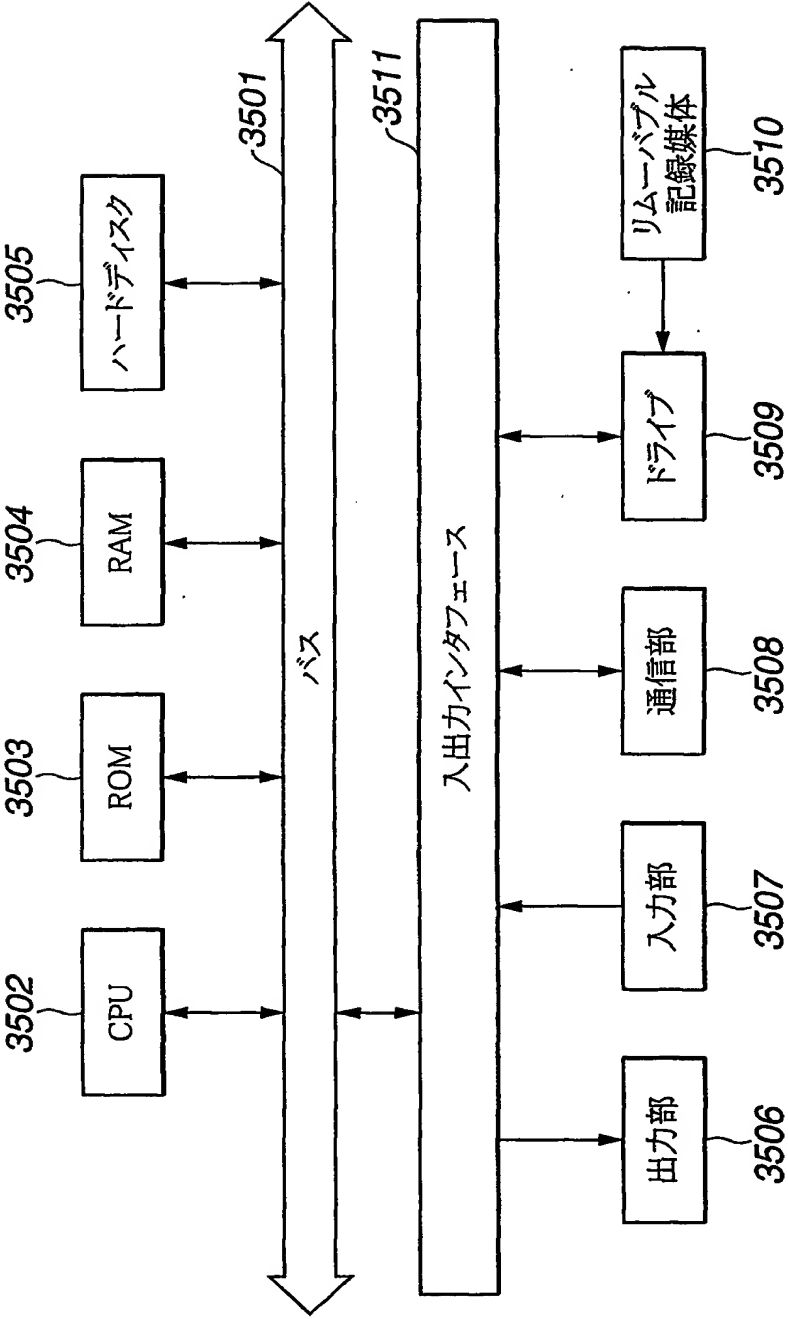


FIG.35

THIS PAGE BLANK (USPTO)

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/00, G11B20/10, G11B20/12

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/00, G11B20/10, G11B20/12, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2001年
 日本国登録実用新案公報 1994-2001年
 日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

WPI, JICST 科学技術文献データベース cipher, encryption, DVD, timestamp

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 11-224456 A (ソニー株式会社) 17.8月.1999(17.08.99), 第10欄第30-42行, 第11欄第40行-第12欄 第2行, 図6 (ファミリーなし)	1-47
A	EP 874503 A2 (Sony CORP.) 28.10月.1998(28.10.98), 第6欄第49行-第7欄第57行 & JP 10-303945 A, 第11欄第34行-第12欄第46行 & KR 98081633 A	1-47
A	EP 924930 A2 (Hitachi, Ltd.) 30.11月.1998(30.11.98), 第9欄第57行-第10欄第44行, 図4, 7 & JP 11-176091 A, 第12欄第36行-第13欄第26行, 図4, 7	1-47

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」口頭による開示、使用、展示等に言及する文献
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」同一パテントファミリー文献

国際調査を完了した日

04.07.01

国際調査報告の発送日

17.07.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正



5M

9364

電話番号 03-3581-1101 内線 3597

THIS PAGE BLANK (USPTO)